Yura: Relaciones internacionales

Departamento de Ciencias Económicas, Administrativas y de Comercio

Revista electrónica ISSN: 1390-9381

N° 11: Julio - septiembre 2017

La ciberseguridad, y su incidencia en las políticas de la seguridad de la información de la Armada del Ecuador. pp. 306 - 323

Almeida Freire, Andrés Lenin.

Universidad de las Fuerzas Armadas ESPE

Sangolquí-Ecuador

Av. General Rumiñahui S/N, Sector Santa Clara- Valle de los Chillos; Sangolquí, Quito.

andres_alm_f1@hotmail.com

La ciberseguridad, y su incidencia en las políticas de la seguridad de la información de la Armada del Ecuador.

Almeida Freire, Andrés Lenin.
Universidad de las Fuerzas Armadas ESPE
andres_alm_f1@hotmail.com

Resumen

El Ecuador actualmente posee un Sistema de Gestión de Seguridad de la Información de la Armada del Ecuador, el cual está encargado de precautelar y velar por la seguridad de los datos, descubrir la penetración de ataques informáticos; así como también ejecutar mecanismos de recuperación en caso de producirse este tipo de eventualidad. Se desarrolló un estudio que se centró en la ciberseguridad y su influencia en las políticas de seguridad de la información de la Armada del Ecuador. Las principales fuentes bibliográficas empleadas fueron documentos de la Subsecretaría del Interior del Ministerio del Interior y Seguridad Pública y la Subsecretaría de Defensa Nacional del Ministerio de Defensa Nacional, trabajos de titulación de tercero y cuarto nivel, artículos científicos, entre otros. La investigación siguió la metodología de la revisión documental y se dividió en tres etapas; búsqueda, selección y análisis de la información. Estos procesos, a partir de publicaciones relevantes identificadas, favorecieron la aproximación a los antecedentes de la ciberseguridad para la conformación de políticas efectivas de seguridad de la Información, mediante la contrastación de esta legislación con aquella que rige los sistemas relacionados con seguridad de la información a nivel nacional y el análisis, con carácter ilustrativo, de algunos ejemplos de los accesos indebidos a la información y de posibles brechas de seguridad, unidos a una serie de consideraciones que tal vez puedan resultar útiles para un futuro análisis sistemático de la ciberseguridad y su influencia en las políticas de seguridad de la información de la Armada del Ecuador. Se concluye que la transcendencia de la ciberseguridad para el diseño de políticas de seguridad de la información es limitada, a pesar de la reciente introducción del Sistema de Gestión de Seguridad de la Información de la Armada del Ecuador. Esto constituye un llamado a la elaboración y el establecimiento de prioridades de investigación en este ámbito.

Palabras clave

Ciberseguridad, seguridad de la información, ciberespacio.

Abstract

Ecuador currently has an Information Security Management System of the Ecuadorian Navy, which must protect and safeguard data, discover computer attacks, as well as to execute mechanisms of recovery in case of any type of eventuality. This study was focused on cybersecurity and its influence on the information security policies of the Ecuadorian Navy. The main bibliographical sources used were documents from the Subsecretaría del Ministerio del Interior y Seguridad Publican and the Subsecretaría de Defensa Nacional del Ministerio de Defensa Nacional, titles of third and fourth level, scientific articles, among others. The research followed the methodology of the documentary review and was divided into three stages: search, selection and analysis of information. These processes, based on relevant publications identified, favored the approximation to the background of cybersecurity for the creation of effective information security policies, by contrasting this legislation with that which governs systems related to information security at national level and the illustrative analysis of some examples of improper access to information and possible security breaches, together with a number of considerations that may be useful for a future systematic analysis of cybersecurity and its influence In the information security policies of the Navy of Ecuador. Finally it is concluded that the transcendence of cybersecurity for the design of information security policies is limited, despite the recent introduction of the Information Security Management System of the Ecuadorian Navy. This is a call for the development and establishment of research priorities in this area.

Keywords

Cybersecurity, information security, cyberspace.

Al considerar el acelerado dinamismo tecnológico aparejado al fenómeno de Internet como medio de comunicación, transmisión y construcción de información, que han caracterizado las últimas décadas, la ciberseguridad resulta un tema de interés prioritario. Esta es entendida como la totalidad de acciones que enrumbadas a asegurar tanto las redes como los sistemas que componen el ciberespacio a partir de tres posturas esenciales: descubriendo y afrontando infracciones, revelando, contestando y recobrándose de sucesos y salvaguardando la confiabilidad, los medios y totalidad de la información (Villalba, 2015). Aunado a ello, y debido al progreso de las relaciones internacionales y los procesos condicionados por la globalización y el desarrollo cibernético, los Estados se encuentran a sí mismos en un riesgo permanente respecto a sus sistemas de defensa. Esto ocurre al producirse nuevas amenazas como el ciberterrorismo, asunto que ha tomado importancia en la agenda de seguridad internacional. (Torres, 2014). A ello no escapa el Ecuador, país que actualmente posee un Sistema de Gestión de Seguridad de la Información de la Armada del Ecuador, el cual está encargado de precautelar y velar por la seguridad de los datos, descubrir la penetración de ataques informáticos; así como también ejecutar mecanismos de recuperación en caso de producirse este tipo de eventualidad.

A partir de la conformación de este sistema, son incuestionables los avances que se han logrado en relación con la ciberseguridad. Un proceso de auditoría habitual se lleva a cabo dentro de los presupuestos de ciberseguridad, con la intención de revelar irregularidades e insuficiencias de este tipo de sistema. Por otro lado, sistemáticamente se constata que los servidores y equipos informáticos y de comunicaciones implicados en el proceso de ciberseguridad conozcan y practiquen las reglas establecidas para planes de contingencia en caso de infracciones internas o de penetraciones externas que comprometan de alguna manera la seguridad y la paz tanto local como nacional (Fuerza Naval Ecuador, 2010). No obstante, se ha comprobado, en este estudio, que estos avances no resultan suficientes para contribuir significativamente a la prevención y erradicación de accesos indebidos a la información y brechas de seguridad que inciden negativamente en contextos tecnológicos, físicos o humanos.

Idealmente podría pensarse que políticas de seguridad de la información se adoptan como secuela de la existencia de evidencia científica, proveída por la investigación. En la práctica se da una constatación concluyente del divorcio entre la problemática de la ciberseguridad y el diseño de las mencionadas políticas. En este sentido, los escasos estudios que abordan la ciberseguridad en Ecuador (Estado Mayor de la Fuerza Naval, 2010; Guagualango y Moscoso, 2011; Pérez, 2012; Andrade y Fuertes, 2013; Delgado, 2014;

Castro, 2015) ponen su acento en dos posiciones, que aunque diferentes no resultan antagónicas, sino complementarias: la defensa cibernética y la integración de la ciberseguridad en las políticas de seguridad de la información.

Es así que algunos investigadores preocupados por la temática alertan al Ministerio de Defensa ecuatoriano sobre la necesidad imperiosa de fundar un Mando de Defensa Cibernética para el resguardo de infraestructuras y servicios púbicos críticos (Ramos, 2014).
Una segunda problemática se asocia a la falta de claridad respecto a la influencia de la ciberseguridad en las políticas de seguridad de la información de la Armada del Ecuador.

¿Por qué podemos afirmar esto? Un reciente estudio prospectivo de la ciberdefensa en las Fuerzas Armadas del Ecuador (Arauz, 2015) señala un conjunto de incongruencias en este sentido: primeramente el Comando de Ciberdefensa ecuatoriano no cuenta con profesionales capacitados en ciberseguridad, aunque sí con experiencia en el manejo de las tecnologías de la comunicación e información. En segundo lugar el aparato legal ecuatoriano no cuenta con regulaciones del uso de internet y redes sociales, situación que deja impune a infracciones ilícitas de vario tipo. Si bien el Código Orgánico Integral Penal contiene sanciones a determinados delitos de orden informático, se requiere de leyes que normen la protección de la información, así como evitar acciones ilegales a través de internet. En tercer lugar, las políticas del Estado ecuatoriano no son claras en regular los mecanismos y respuestas ante ataques de orden cibernético y por último existe un vacío de convenios internacionales entre los países que conforman UNASUR, en torno a implantar estrategias comunes de ciberseguridad.

Con base en lo aquí descrito el presente estudio se centra en el análisis de la ciberseguridad y su influencia en las políticas de seguridad de la información de la Armada del Ecuador. Este trabajo añade valor a la literatura existente en dos direcciones, en primer lugar, sus hallazgos poseen implicaciones tanto para la práctica como para la paulatina instauración de modelos más pertinentes de ciberseguridad en la Armada del Ecuador que coadyuven a visibilizar su influencia en las políticas de seguridad de la información. Por otro lado, las reflexiones realizadas concernientes a la contrastación de la legislación a nivel de las Fuerzas Armadas con aquella que rigen los sistemas relacionados con seguridad de la información a nivel nacional pueden resultar de utilidad, al permitir que los generadores de políticas y normativas ganen en comprensión en cuanto a la necesidad de que se inserte, en mayor medida, la ciberseguridad en las mismas.

Materiales y Métodos

La investigación siguió la metodología de la revisión documental y se dividió en tres etapas; búsqueda, selección y análisis de la información. Estos procesos favorecieron la aproximación a los antecedentes de la ciberseguridad para la conformación de políticas efectivas de seguridad de la Información, mediante la contrastación de esta legislación con aquella que rige los sistemas relacionados con seguridad de la información a nivel nacional y el análisis, con carácter ilustrativo, de algunos ejemplos de la influencia creciente de los accesos indebidos a la información y de posibles brechas de seguridad en las políticas de seguridad de la información, unidos a una serie de consideraciones que tal vez puedan resultar útiles para un futuro análisis sistemático de la ciberseguridad y su influencia en las políticas de seguridad de la información de la Armada del Ecuador.

Respecto al procedimiento para el tratamiento y el análisis de información, de acuerdo a una variación de la metodología propuesta por Gómez, Fernando, Aponte y Betancourt (2014); se delimitó el material informativo como libros, revistas de investigación científica y sitios Web.

Seguidamente se definió el dominio de la investigación y se emplearon ecuaciones de búsqueda, atendiendo a las siguientes palabras clave y operadores lógicos: “ciberseguridad AND políticas de seguridad de la información de la Armada del Ecuador”, “ciberseguridad AND ciberdefensa”, “políticas de seguridad de la información de la Armada del Ecuador OR normativa legal de ciberdefensa”, se incluyeron términos específicos del tema a investigar en idioma inglés “ Cyber security AND information security policies of the Army of Ecuador”

Posteriormente fueron aplicados criterios de selectividad que favorecieron, al equipo de investigación, centrarse en los documentos relevantes. Se procedió a organizar de manera sistemática la documentación encontrada, mediante el uso del programa Reference Manager; quedando así la información agrupada y clasificada según el tipo de documento, el título, los autores y su aporte.

A continuación se resumieron aspectos como número de documentos por año, documentos, citaciones por autor, documentos e investigaciones realizadas por país, entre otros.

Las principales fuentes bibliográficas empleadas fueron documentos de trabajo de la Subsecretaría del Interior del Ministerio del Interior y Seguridad Pública y la Subsecretaría de Defensa Nacional del Ministerio de Defensa Nacional, trabajos de titulación de tercero y cuarto nivel, artículos científicos, entre otros. Teniéndose que de los 50 documentos iniciales, 40 fueron identificados como de mayor interés. Estos, a su vez, fueron filtrados y leídos con

mayor detalle, seleccionándose 35 de verdadera relevancia para la investigación. Luego de ejecutarse la lectura detallada, finalmente se descartaron 3 artículos y se eligieron 32 trabajos, a partir de los cuales se elaboró el estado del arte sobre el tema.

Resultados

Antecedentes de la ciberseguridad para la conformación de políticas efectivas de seguridad de la Información

En la literatura es recurrente encontrar que los problemas de ciberseguridad son un determinante de las intervenciones y en una de las causas de la mejora de la ampliación o revisión de las políticas de seguridad de la información. No obstante, a menudo se plantean dificultades para evaluar su impacto sobre las mismas, ya que la atribución de una asociación causal entre la ciberseguridad, la conformación de políticas efectivas de seguridad de la Información y su correcta aplicación carecen de suficiente evidencia empírica.

Varios estudios han destacado la influencia de un eficaz sistema de ciberseguridad para la creación de políticas efectivas de seguridad de la información. Riquelme (2012) retoma el concepto de Guerra de la Información (GI), perteneciente al Departamento de Defensa de los Estados Unidos, el más admitido teóricamente por los sistemas de fuerzas armadas en el planeta, y que se relaciona con acciones realizadas con el objetivo de alcanzar ventaja en el acceso y manejo de determinada base de datos; para implicarlo tanto en los procesos como en los sistemas afines de sus contrarios, al mismo tiempo para resguardar la información, así como los procesos y sistemas propios que toman a la información como base.

Por su parte, Vargas (2014) al ahondar en el sistema de seguridad nacional colombiano, recalca la potencial inversión del "poderío blando" físico de un país en conflicto bélico a otro poder hegemónico mediante un óptimo dominio del ciberespacio.

Sánchez (2012) conceptualiza tres términos de aceptada aplicación en los estudios sobre las Políticas de Seguridad de la Información: el cibercrimen, el ciberterrorismo y la ciberguerra. El primero contiene a una serie de infracciones de orden informático y económico (piratería comercial, computer hacking) orientadas a la penetración de estados de intimidad, así como a la socialización de mensajes ilícitos y perjudiciales y a la invitación a la prostitución y al crimen organizado. El segundo se relaciona con las estrategias por medio de las cuales el terrorismo usa las tecnologías de la información para amedrentar, obligar u originar daños a determinada sociedad con objetivos político-religiosos; mientras que el

tercero se vale de todo el instrumental electrónico e informático para destruir los sistemas electrónicos y de comunicación del contrincante y conservar los propios en óptimo funcionamiento.

Un estudio realizado por Leiva (2015) evalúa la Estrategia Nacional de Ciberseguridad (ENCS) en trece países de cuatro continentes, donde se define como uno de sus componentes a las denominadas capacidades cibernéticas militares, o sea, la posibilidad de la armada de una nación para precautelar y neutralizar toda agresión o hecho de procedencia cibernética que incida negativamente en la protección de su soberanía.

Otra investigación ejecutada en España (Amich y Velázquez, 2014) destaca la importancia de aumentar y perfeccionar de forma permanente las capacidades de ciberdefensa de las Fuerzas Armadas que faciliten una apropiada defensa de sus redes y sistemas de información y telecomunicaciones, así como también de otros sistemas que perjudiquen a la defensa del país.

Queiroz (2015), al analizar la Estrategia Nacional de Defensa (END) en el contexto brasileño, enumera tres sectores medulares que sustentan el desarrollo de la defensa nacional: el concerniente a la energía nuclear, el espacial y el cibernético. Para este Ministerio de Defensa, la implementación de estrategias para la efectividad de un sistema defensivo cibernético ha devenido una exigencia de máxima atención para que tanto la Armada, como la Fuerza Aérea y el Ejército logren una sincronía mediante la utilización de redes comunes. A nivel operativo, está la importancia de las operaciones conjuntas coordinadas por el Estado Mayor Conjunto de las Fuerzas Armadas.

Dichos enfoques muestran una directriz teórica común y a tomar en cuenta: si bien las maniobras ofensivas de la guerra cibernética no tienen esencia cinética, posibilitan potenciales afectaciones a grupos humanos, así como secuelas físicas irremediables. Un punto de giro en la atención a la ciberseguridad lo constituyó la aparición en la célebre revista inglesa The Economist, de su editorial "Cyberwar", en julio de 2010, que reconocía el riesgo de la extensión de la innovación digital hacia el nuevo concepto de ciberataque o de ciberejército. (The Economist, 2010). Jeffrey Carr (2010) relata ejemplos de ciberguerra ocurridos en los siglos XX y XXI, y menciona los siguientes: China, Israel, Rusia (incluye en este acápite los casos de la Segunda Guerra Rusia-Chechenia del periodo 1997-2001; la ciberguerra de Estonia (2007) y la Guerra Rusia-Georgia (2008)), Irán y Corea del Norte.

En la administración de Obama, EE. UU. comenzó a entender a la infraestructura digital americana como activo estratégico nacional. The Economist deja entrever otra potencial problemática producto de una ruptura del sistema de comunicaciones a nivel

planetario. Si se tiene en cuenta que dicha rotura resulta improbable que se lleve a cabo gracias a las múltiples estrategias de trasmisión de datos por Internet, se puede aseverar que en algunos puntos la infraestructura digital global se puede quebrar. Más de las nueve décimas partes del tráfico de Internet utilizan la vía submarina mediante cables compuestos por fibra óptica, que alcanzan su nivel más vulnerable en las zonas siguientes: bordeando Nueva York, el Mar Rojo o el estrecho de Luzón en Filipinas. Otras dificultades reales que alerta dicha publicación guardan relación con la inconsistencia de algunos gobiernos en ciertas zonas africanas que pueden dar al traste con la creación de amparos para los cibercriminales. (Joyanes, 2011)

En síntesis, a pesar de que contar con leyes adecuadas para los delitos informáticos, las infraestructuras críticas y la protección de datos resultan cruciales para la ciberseguridad, no se ha privilegiado el desarrollo de un marco jurídico adecuado, basado en precedentes tomados de acuerdos internacionales y de la legislación de otros países.

Reflexiones sobre la influencia creciente de los accesos indebidos a la información y posibles brechas de seguridad en las políticas de seguridad de la información.

Las amenazas cibernéticas que podrían afectar la seguridad interna y externa del Estado ecuatoriano ganan cada vez más peso, y han ido interviniendo progresivamente en las políticas de seguridad de la información. Seguidamente se ilustra la influencia creciente de los accesos indebidos a la información y posibles brechas de seguridad; tanto físicas, tecnológicas y humanas, en dichas políticas.

Ante la definición de gobernanza de internet brindada por la Cumbre Mundial sobre la Sociedad de la Información (Túnez, 2005), entendida como el progreso y ejecución a cargo de directivas gubernamentales, así como del sector privado y de la sociedad civil, en sus papeles respectivos, de normativas, políticas y leyes que regulen la toma de decisiones y de programas que permitan la evolución y utilización de Internet (Delgado, 2014); se pueden considerar como potenciales brechas de seguridad que incidan negativamente en contextos tecnológicos, físicos o humanos ecuatorianos a las siguientes situaciones:

1. Al prevalecer en Ecuador el uso de la telefonía móvil resulta imprescindible la evaluación de la incidencia de esta clase de infraestructura de acceso en cuanto a aquellas directrices que tienen relación con la protección de la privacidad. La tecnología móvil, al utilizar estándares cerrados permite que su firmware no pueda ser accesible, aunque en

territorio ecuatoriano se exija un registro de carácter ineludible de la totalidad de los dispositivos móviles. Dicha problemática puede provocar infracciones reales a sistemas de seguridad y comunicación y las consecuentes privacidad y libertad de expresión. Por lo tanto, la práctica y cumplimiento de los derechos humanos pueden verse afectados por sanciones de tipo legal, agresiones remotas e implicación en ataques de terceros. (Delgado, 2014)

2. Teniendo en cuenta que varias empresas locales proveedoras de servicios de Internet en Ecuador así como también instituciones gubernamentales y académicas usan IPv6 e IPv4; actualmente la generalidad de usuarios se conecta a Internet dentro de sub-redes dirigidas por los proveedores de servicio, a través de soluciones denominadas "parche", como los mecanismos NAT y CIDR. Dicha situación implica que un equipo en la jurisdicción del territorio ecuatoriano cuenta con el acceso a Internet público, no así Internet tiene acceso a ese equipo, al menos no de tipo directo; contexto que compromete el principio de extremo a extremo y la integridad de los sistemas de información y comunicación (Klein, 2014).

3. Una investigación realizada en el año 2009 toma como objeto la red inalámbrica del Laboratorio DELTA de la ESPOL, y comprueba determinadas brechas de seguridad mediante el programa NetStumbler. La ausencia de conciencia sobre la importancia de la información manejada por el personal del laboratorio; así como la incomunicación del mismo con la directiva gerencial, provocan la intrusión de agentes externos. (Castillo, Cabezas y Escalante, 2009). Este ejemplo puede extrapolarse a contextos macro e inclusive, a nivel de país.

4. Otro estudio (Pérez, 2012) evalúa los sistemas de seguridad de las cuentas nacionales del Banco Central del Ecuador y basándose en la norma ISO/IEC 27001 analiza varias brechas en la seguridad de la entidad condicionadas por: poca responsabilidad de la directiva con los sistemas de seguridad de la información, poca capacitación al personal implicado en los sistemas de seguridad de la información, en el orden de la actualización obligatoria sobre manejo de tecnología asociada y de protocolos de seguridad nacional e internacional, ausencia de un foro funcional transversal para la implementación de políticas de seguridad y la poca estructuración de las responsabilidades en torno a la protección de activos.

5. Según Andrade y Fuertes (2013) se ha incrementado el número de ataques informáticos en Ecuador que persiguen como objetivo extraer información personal, ejecutar agresiones de denegación de servicio, ejecutar estafas con tarjetas de crédito o destruir la

reputación de una institución o empresa. Bajo este contexto las organizaciones se han visto abocadas al desarrollo de sus sistemas de seguridad de la información, y nos solo adquirir arquitectura de seguridad como firewalls, herramientas antivirus y anti-spam.

6. Guagualango y Moscoso (2011) evaluaron la seguridad informática del Data Center de la Escuela Politécnica del Ejército y descubren que en principio se incumple con la Norma ISO 27004; los implicados en el sistema de seguridad desconocen en gran medida las políticas que lo regulan, ante la ausencia de documentos, normativas y procedimientos, así como un responsable de la creación, actualización y aplicación de dichas políticas; falta de controles asiduos para constatar la efectividad de las políticas; ausencia de roles que definan el accionar del personal de seguridad; ausencia de condiciones contractuales de seguridad con terceros y outsourcing.

En general, se reconozca que la influencia de la ciberseguridad sobre la normativa es limitada, es evidente también que tiene mucho que ver en el diseño de políticas de seguridad de la información. Seguidamente se contrasta la legislación a nivel de las Fuerzas Armadas con aquella que rige los sistemas relacionados con seguridad de la información a nivel nacional.

En lo que respecta a la legislación relacionada con seguridad de la información a nivel de Ecuador, varios aparatos legales sustentan estas políticas en el contexto ecuatoriano. Es así que la Constitución del Ecuador en su Sección undécima, titulada “Seguridad humana” y específicamente en su Artículo 393 (Asamblea Constituyente, 2008, p. 176). De igual modo, la Ley Orgánica de Transparencia y Acceso a la Información Pública (2004-24), en su Artículo 17 establece directrices que impiden el derecho al acceso a la información pública (Congreso Nacional, 2004, p. 10).

El Artículo no. 2 de la Ley Orgánica de la Defensa Nacional (2007-14) postula que las Fuerzas Armadas, como componente de la fuerza pública, persiguen los siguientes objetivos: mantener la soberanía nacional; proteger la integridad, la unidad e independencia del Estado; garantizar el ordenamiento jurídico y democrático del estado social de derecho y colaborar con el desarrollo social y económico del país; podrán participar en actividades económicas relacionadas únicamente con la defensa nacional e intervenir en los demás aspectos concernientes a la seguridad nacional de acuerdo con la ley (p. 1). En el capítulo IV “Del Comando Conjunto de las Fuerzas Armadas” se enumeran varias atribuciones que tienen

relación directa con el protagonismo de estas fuerzas en la elaboración de políticas de seguridad de la información (p. 3).

Por su parte, ante la urgencia de adecuar la doctrina de seguridad al mundo contemporáneo, en aras de implementar un nuevo Sistema de Seguridad Integral mediante un enfoque civilista y diacrónico para el nuevo contexto geopolítico internacional; la Ley de Seguridad Pública y del Estado (2009) demanda que la salvaguardia de la soberanía del Estado y la integridad del territorio tendrá como componentes esenciales al Ministerio de Defensa y al de Relaciones Exteriores en los contextos de su compromiso y competencia. Corresponde a las Fuerzas Armadas su ejecución para cumplir con su misión fundamental de defensa de la soberanía e integridad territorial. (p. 7).

Respecto a la legislación relacionada con seguridad de la información a nivel de las Fuerzas Armadas, puede afirmarse que al contar con férreas políticas de seguridad de la información, la Armada del Ecuador detecta y controla los riesgos cibernéticos de disímil tipología y procedencia. Estas prácticas rectoras son revisadas y actualizadas desde la visión de la ciberseguridad.

Con el objetivo de informar al individuo (técnicos y administrativos) en su calidad de usuario del Sistema de Comunicaciones de la Armada ecuatoriana, en función de proteger la infraestructura tecnológica y digital, las políticas de seguridad de la información incluyen una normativa que estipula lo permitido o no en la utilización tanto de la red constituida como de los diversos servicios tecnológicos.

En el caso de las políticas implementadas por las estructuras del Sistema de Comunicaciones Navales (SCN) de la Armada ecuatoriana, incluyen seis directrices en el diseño de su proceso de comunicaciones e informático, que a continuación se detallan por su pertinencia: disponibilidad, utilidad, integridad, autenticidad, confidencialidad y posesión (Fuerza Naval Ecuador, 2010).

Con base en el estándar ISO/IEC 27002:2005, el sistema de seguridad del SCN ecuatoriano, para conformar una normativa legal interna que regule las políticas de seguridad de la información y de las comunicaciones, ha decidido cumplir con los siguientes dominios: políticas de seguridad con carácter obligatorio, procesos organizativos, y gestión de activos. Mencionadas estas disposiciones generales, es preciso declarar que son aplicables a contextos o materiales de diversa índole y que se convertirán en individuales según las acciones que amerite cada sistema, tomando en cuenta el nivel de precaución, así como el impacto de ataques cibernéticos de plural naturaleza.

Discusión

Como la sociedad contemporánea resulta cada más dependiente de la tecnología, la influencia de esta última en el efectivo funcionamiento de los Estados, y específicamente de sus fuerzas armadas, cuerpos de seguridad e infraestructuras, se constata cada vez mayor, por lo que, por consiguiente, la innovación futura aumentará esta incidencia.

En base a los resultados de la revisión puede afirmarse que las tecnologías de la información permiten generalmente con efectividad el funcionamiento de los sistemas de seguridad de la información y de la comunicación de las fuerzas armadas, compuestos por el basamento logístico, el mando y examen sostenido de sus fuerzas, así como los datos relacionados con la inteligencia en tiempo real. Toda esta infraestructura se supedita a redes informáticas y de comunicaciones. En menos de una generación, las TIC en el contexto militar han progresado desde un simple instrumento para optimizar la productividad administrativa a un mecanismo de defensa estratégico. (Díaz del Río, 2011).

En este sentido, las intenciones de orden intelectual o económicas que sustentaban a los ataques cibernéticos han mutado en los últimos años a objetivos centralmente políticos, por lo que sus efectos ya no solo acarrean una pérdida económica, sino en las contiendas entre naciones que ostentan y evalúan sus fuerzas, en torno a las directrices de tierra, mar, aire y espacio, mediante el ciberespacio.

La investigación realizada, como se ha planteado anteriormente, muestra los aportes de varios países que incluso han creado sistemas de ciberseguridad de la información y de la comunicación: en Estados Unidos la seguridad en el ciberespacio representa la misma importancia que el denominado “Homeland Security”, pues mediante un coordinador de ciberseguridad en la Casa Blanca, se controlan las tácticas nacionales para garantizar los intereses de los americanos en el ciberespacio. Por su parte, Alemania ha conformado la Unidad de Reconocimiento Estratégico del Bundeswehr, compuesta por varios especialistas en seguridad y en el Reino Unido se ha fundado una Oficina de Ciber Seguridad (OCS, Office of Cyber Security) que tiene como función coordinar las capacidades de defensa y de respuesta a intromisiones en redes (Díaz del Río, 2011).

Otra problemática acuciante en la conformación efectiva de sistemas internacionales de ciberseguridad es entrevista por Casar (2012) al evaluar las acciones de organismos aglutinadores y canonizantes desde el punto de vista político, económico y militar, como la ONU, la OTAN, la OCDE, la UIT y la UE. El autor, con quien concordamos, defiende la postura de la existencia de una fragmentación provocada por el objetivo de cada organismo internacional, posición de índole natural que aboga por el cumplimiento y la satisfacción de

los fines para lo que fueron fundadas, razón por la que no se ha establecido una integridad en temas de ciberseguridad.

Según Domínguez (2016) los modelos teóricos del campo científico de la Criminalística deben redefinirse en el sentido de una nueva actuación que toma como base mecanismos de pensamiento ante la posibilidad de agresiones, ataques y conflictos ya en el amplio contexto de lo cibernético. Dicha postura, a la cual nos adscribimos, implica la búsqueda de estrategias que permitan a los sistemas de ciberseguridad conocer y aplicar los enfoques del aparato criminal, es decir, inspeccionar las posibles maniobras de operación de supuestos atacantes, y estar dispuestos a adivinar los teatros de sus actuaciones. Si no se da importancia a esta perspectiva, se estaría incurriendo en una dinámica de reacción, por lo que se propone otras de tipo proactivo, o sea, de anticipación, de organizarse para no ser afectado por los efectos de esta clase de ataques en la red.

Desde un enfoque jurídico, tomamos partido por el criterio de Robles (2016), este afirma que el Derecho Internacional no ha tomado en cuenta realmente al ciberespacio como el resto de componentes físicos, ni de su estructuración, ni de su régimen jurídico. Teniendo en cuenta que su función persigue el ordenamiento de competencias al constituirse como espacio genéticamente mundial, que se suma y transversaliza a los anteriores porque además resulta estructural y funcionalmente global, no lo ha ejecutado. “No es un simple problema de organización de las competencias, como en el resto de los dominios, sino que se trata de ordenar la coexistencia social en un espacio diferente de sus predecesores y con una extraordinaria capacidad de interacción y de afectación de los mismos.” (p. 4)

De igual modo se coincide con De Tomás (2014), quien aboga en otro ámbito, el universitario, por la consolidación de una cultura de ciberseguridad, que necesita consecuentemente de un reforzamiento de la cimentación de otra cultura de seguridad y defensa que promueva una intervención de la totalidad de sectores mediante una importante empresa de desarrollo y comunicación para que principios, valores y derechos constitucionales (conciencia nacional) alcancen real valor.

Junto al hecho de identificar las amenazas cibernéticas potenciales y la disposición a defenderse desde esta perspectiva, sin dar lugar a la interpretación; se exhorta al establecimiento de una conciencia de ciberseguridad que facilite dar respuestas de manera efectiva, conveniente y genuina a la amenaza cibernética que puede poner en peligro los principios y valores democráticos o, incluso, la propia continuidad del Estado.

La problemática teórica que gira en torno al campo de la Ciberseguridad, sin dudas ha influenciado las estrategias de conformación de Políticas de Seguridad de la Información de la Armada del Ecuador, trayendo consigo sus propias implicaciones teórico-prácticas.

Por último, los Centros de Tecnologías de la Información de la Armada ecuatoriana, teniendo en cuenta la ingente preocupación de los organismos del Estado ante la posibilidad de ser objetos de ataque de orden cibernético, establecen las siguientes directrices:

1. Mantener configuraciones de equipos, dispositivos y demás componentes conforme a su función y responsabilidad, que permitan la conectividad y provisión de los servicios de tecnologías de la información a los repartos armados a nivel nacional y desde una perspectiva de seguridad.

2. Monitorear los servicios de Internet, correo electrónico, con el objetivo de garantizar su eficiencia y seguridad y constatando que cumplan con los requerimientos de seguridad de la información y controlar que el personal de mantenimiento de cada Centro de Tecnología de la Información, instale, configure y actualice el software de gestión operativo y administrativo en el equipamiento propio de la institución.

3. Verificar que se dé cumplimiento a los procedimientos de respaldo de los sistemas de seguridad de la información y la comunicación y verificar que se cumpla con el mantenimiento de los equipos informáticos y de comunicación de datos, en función de dar cumplimiento a las directrices estipuladas en los sistemas de ciberseguridad de la información.

4. Verificar que los servidores y equipos informáticos y de comunicaciones se encuentren situados en espacios físicos adecuadamente administrados, y que estén bajo condiciones ambientales apropiadas, medios de seguridad lógica y física consecuentes con los necesarios planes de contingencia en situaciones de ataque cibernético (Fuerza Naval Ecuador, 2010).

A modo de conclusión, como se ha visto hasta aquí, la transcendencia de la Ciberseguridad para el diseño de políticas de seguridad de la información es limitada, a pesar de la reciente introducción del Sistema de Gestión de Seguridad de la Información de la Armada del Ecuador. Lo cual constituye un llamado a la elaboración y el establecimiento de

prioridades de investigación en este ámbito, ya que este sistema adolece de una orientación investigativa que permita justificar científicamente las propuestas de normativas e intervenciones, introduciendo elementos de racionalidad a la hora de incorporar en la práctica los resultados de las investigaciones realizadas en esta dirección, de manera que ello redunde en la adopción de enfoques más integrales sobre la ciberseguridad y en el fortalecimiento la regulación para asegurar los sistemas de información y la cooperación internacional en ciberseguridad.

En suma, existen un conjunto de aspectos no resueltos, sobre los cuales ha arrojado luz este estudio. Aunque la Armada del Ecuador cuenta con políticas de seguridad revisadas y actualizadas desde la visión de la ciberseguridad, pueden ocurrir potencialmente accesos indebidos a la información y posibles brechas de seguridad; tanto físicas como tecnológicas y humanas, que podrían afectar la seguridad interna y externa del Estado ecuatoriano, ante lo cual adquieren un valor esencial las tres directrices esenciales sobre ciberseguridad: descubrir y afrontar infracciones, revelar, contestar y recobrarse de sucesos y salvaguardar la confiabilidad, los medios y la totalidad de la información.

El análisis realizado posibilitó aglutinar un conjunto de evidencia científica que reafirme la importancia de la valoración de la ciberseguridad, y su influencia en las políticas de seguridad de la información de la Armada del Ecuador. En la medida en que se cuente con investigaciones que muestren la variedad de prácticas que se han desarrollado en este ámbito y sus efectos positivos, se aportará evidencia que permita sustentar un enfoque teórico-práctico integrador de la Ciberseguridad en la Armada del Ecuador. Por tanto, es factible proponer la apertura de nuevas líneas de investigación que intenten situar el papel de la investigación en el contexto de la planificación y el diseño de políticas de seguridad de la información, de manera que se destaque la transcendencia de los distintos enfoques de la ciberseguridad, y se consiga apuntar al papel integrador que tal vez se podría desarrollar desde la investigación de la ciberseguridad y sus efectos en las políticas de seguridad de la información

Referencias bibliográficas

Amich, C. y Velázquez, A. P. (2014). La ciberdefensa y sus dimensiones global y específica en la estrategia de seguridad nacional española. *Icade. Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales*, (92), 50-76.

Andrade, R. y Fuertes, W. (2013). *Diseño y dimensionamiento de un equipo de un equipo de respuesta ante incidentes de seguridad informática (CSIRT). Caso de estudio: ESPE*. Recuperado de: http://ciencia.espe.edu.ec/wp-content/uploads/2013/05/COM61.pdf

Asamblea Constituyente. (2008). *Constitución del Ecuador*. Recuperado de: http://www.asambleanacional.gob.ec/sites/default/files/documents/old/constitucion_de_bolsillo.pdf

Asamblea Nacional. (2009). *Ley de Seguridad Pública y del Estado*. Recuperado de: http://www.asambleanacional.gov.ec/documentos/Ley-de-Seguridad-Publica-y-del%20Estado.pdf

Carr J. (2010). *Cyber Warfare. Sebastopol*, USA: O´Reilly.

Casar, J. R. (2012). *El ciberespacio. Nuevo escenario de confrontación*. España: Centro Superior de Estudios de la Defensa Nacional.

Castillo, A., Cabezas, R. y Escalante, J. *Consultoría para la determinación de brechas de seguridad en una red inalámbrica* [tesis de grado]. Escuela Superior Politécnica del Litoral, Guayaquil.

Castro, E. J. (2015). *Estudio prospectivo de la ciberdefensa en las Fuerzas Armadas del Ecuador* [tesis de especialidad]. Universidad de las Fuerzas Armadas ESPE, Sangolquí, Ecuador.

Congreso Nacional. (2004). *Ley Orgánica de Transparencia y Acceso a la Información Pública*. Recuperado de: http://www.seguridad.gob.ec/wp-content/uploads/downloads/2015/04/ley_organica_de_transparencia_y_acceso_a_la_informacion_publica.pdf

Congreso Nacional. (2007). *Ley Orgánica de la Defensa Nacional*. Recuperado de: http://www.defensa.gob.ec/wp-content/uploads/downloads/2012/07/LEY_ORGANICA_DE_LA_DEFENSA_NACIONAL.pdf

Cyberwar. (2010). *The Economist, 396*(8689), 2.

De Tomás, S. (2014). Hacia una cultura de ciberseguridad: capacitación especializada para un "proyecto compartido". Especial referencia al ámbito universitario. *Icade. Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales*, (92), 13-47.

Delgado, J. A. (2014). *Gobernanza de Internet en Ecuador: infraestructura y acceso.* Recuperado de: http://repositorio.educacionsuperior.gob.ec/bitstream/28000/1579/1/Gobernanza%20de%20Internet%20en%20Ecuador.pdf

Díaz del Río, J. J. (2011). *La ciberseguridad en el ámbito militar*. Recuperado de: https://dialnet.unirioja.es/descarga/articulo/3837348.pdf

Domínguez, J. (2016). La ciberguerra como realidad posible contemplada desde la prospectiva. *Revista de Pensamiento Estratégico y Seguridad CISDE*, 1(1), 18-32.

Estado Mayor de la Fuerza Naval. (2010). *Seguridad de la información*. Quito: Fuerza Naval Ecuador.

Gómez Luna, E., Fernando Navas, D., Aponte Mayor, G.y Betancourt Buitrago, L.A. (2014). Metodología para la revisión bibliográfica y la gestión de información de temas científicos, a través de su estructuración y sistematización. *DYNA.* 81(184),158-163. Recuperado de: https://dx.doi.org/10.15446/dyna.v81n184.37066

Guagualango, R. N. y Moscoso, P. E. (2011). *Evaluación técnica de la seguridad informática del Data Center de la Escuela Politécnica del Ejército* [tesis de grado]. Escuela Politécnica del Ejército, Sangolquí, Ecuador.

Joyanes, L. (2011). Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. *Cuadernos de estrategia*, (149), 11-46.

Klein, D. (2014, julio 30). *Querida #NETMundial, la Gobernanza es genial y todo, pero necesitamos EXIGIR el IPv6 ¡AHORA!* (J. A. Delgado, Trans.) Recuperado de: http://www.aperturaradical.org/

Leiva, E. (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.

Pérez, A. F. (2012). *Diseño y ensayo del Sistema de Gestión de la Seguridad de la Información Estadística (SGSIE). Caso de aplicación: cuentas nacionales en el Banco Central del Ecuador* [tesis de maestría]. Escuela Politécnica Nacional, Quito.

Ponce, A. (2017). *Un acercamiento geopolítico a la ciberseguridad*. México: Instituto de Investigaciones Estratégicas de la Armada de México.

Queiroz, V. J. (2015). *La estrategia de Argentina y Brasil para la Defensa Cibernética, un análisis por los niveles de la conducción* [tesis de especialidad], Instituto Universitario del Ejército, Buenos Aires.

Ramos, M. (2014). *Acerca de la soberanía del Ecuador en el ciberespacio*. Quito: Centro Andino de Estudios Estratégicos.

Riquelme, E, J. (2012). *La influencia de la Guerra de la Información en un Teatro de Operaciones* [tesis de especialidad]. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas, Argentina.

Robles, M. (2016). El ciberespacio: Presupuestos para su ordenación jurídico-internacional. *Revista Chilena de Derecho y Ciencia Política*, *7*(1), 1-43.

Sánchez, G. (2012). Cibercrimen, ciberterrorismo y ciberguerra: los nuevos desafíos del S. XXI. *Revista Cenipec*, (31), 239-267.

Torres, J. A. (2014). *Análisis de la influencia del fenómeno del Ciberterrorismo en las dinámicas de seguridad de la Unión Europea* [tesis de pregrado]. Universidad Colegio Mayor de Nuestra Señora del Rosario, Bogotá.

Vargas, E. M. (2014). *Ciberseguridad y ciberdefensa: ¿qué implicaciones tienen para la seguridad nacional?* [tesis de especialidad]. Universidad Militar Nueva Granada, Bogotá.

Villalba, A. (2015). La ciberseguridad en España 2011 – 2015. Una propuesta de modelo de organización [tesis doctoral]. Universidad Nacional de Educación a Distancia, Madrid.