"ANÁLISIS SISTEMÁTICO DE METODOLOGÍAS Y MODELOS PARA LA GESTIÓN DEL RIESGO EN LAS OPERACIONES NAVALES Y COSTERAS DE REPÚBLICA DOMINICANA"

Systematic Analysis of Methodologies and Models for Risk Management in Naval and Coastal Operations of Dominican Republic

Recibido: 26 / 08 / 2019 Aprobado: 31 / 10 / 2019

Capitán de Fragata
Fausto R. Richardson H.
Armada de República Dominicana

En la actualidad el autor está en la fase de defensa de la tesis de un Doctorado en Proyectos con la Universidad Internacional Iberoamericana (UNINI – México). Asimismo, está cursando una Maestría en Ciberseguridad con triple titulación, del IMF Business School, la Universidad Camilo José Cela y la Universidad de Nebrija. Obtuvo su formación inicial con una Licenciatura en Informática en la Universidad Pedro Henríquez Ureña (UNPHU), en el año 2003. Ha fortalecido sus conocimientos a través de la titulación de Máster en Gestión Universitaria con la Universidad de Alcalá, España, en el año 2015; y una Maestría en Sistemas de Información mención Gestión de la Información con el Stevens Institute of Technology, USA, para el año 2011. También cuenta con diversas especialidades, entre ellas: Especialidad en Derechos Humanos y Derecho Internacional Humanitario (2011) y una especialización en Seguridad Nacional relacionada a la Ciberseguridad (2018). En su formación técnica profesional domina aspectos de Ingeniería de Software, las Redes y la Ciberseguridad. faustorichardson@gmail.com

RESUMEN

Con la llegada del siglo XXI, y el auge que ha tomado la adopción del uso de las Tecnologías de la Información y Comunicación (TIC) en todos los escenarios de la vida diaria de las naciones, las Fuerzas Armadas han llevado sus operaciones a un nuevo escenario de conflicto armado el cual viene acompañado de amenazas que pretenden vulnerar la Seguridad y Defensa Nacional. Este nuevo escenario es el ciberespacio. En ese sentido, las operaciones navales y costeras no han quedado exentas de ser un blanco de ataque de las ciberamenazas que se convierten en un desafío para las fuerzas militares que se encargan de velar de cualquier intento o situación que ponga en riesgo la soberanía nacional. Por lo que el presente artículo pretende analizar de manera sistemática las diferentes metodologías y modelos existentes, como buenas prácticas, para gestionar el tratamiento a los diferentes riesgos cibernéticos que pudieran impactar de manera negativa en el buen desenvolvimiento de las operaciones navales y costeras de República Dominicana.

Palabras clave:
Operaciones navales, riesgos cibernéticos, análisis de riesgos, ciberseguridad.

ABSTRACT

With the arrival of the 21st century, and the boom of the use of Information and Communication Technologies (ICT) in all scenarios in the daily life, the Armed Forces have carried out their operations to a new scenario of armed conflict which is accompanied by threats intended to violate National Security and Defense. This new scenario is cyberspace. In that sense, naval and coastal operations have not been exempt from being a target of cyber threats that become a challenge for military forces that are responsible for overseeing any attempt or situation that jeopardizes national sovereignty. Therefore, this article intends to systematically analyze the different methodologies and models that exist as good practices, to manage the treatment of the different cyber risks that have a negative impact on the smooth development of naval and coastal operations in Dominican Republic.

Keywords:
Naval operations, cyber risk, risk analysis, cybersecurity.

INTRODUCCIÓN

En los últimos años, los diferentes escenarios de la guerra han sido conquistados por un nuevo enfoque o dimensión, gobernado por bits (cero y uno), conocido como ciberespacio. Esta nueva (y para muchas naciones vieja) dimensión se ha convertido en un gran desafío para los Estados, dado su rápida evolución, y la necesidad imperante del uso de herramientas tecnológicas para la automatización de procesos que permiten ser más competentes a las naciones en un mundo gobernado por la globalización.

En ese sentido, ante este nuevo escenario de conflicto armado, donde accionan actores estatales y no estatales, tal como señala Giudici (2013, p.1), estos pueden valerse de los medios electrónicos disponibles, para poner en riesgo la defensa y seguridad de una nación, atacando las vulnerabilidades de las plataformas tecnológicas e infraestructuras críticas de un Estado.

Las operaciones navales y costeras no han estado exentas de los ataques cibernéticos que se han llevado a cabo, por lo que es una necesidad adoptar las buenas prácticas que permitan garantizar la defensa y seguridad de República Dominicana en los aspectos tratados en este artículo.

Por tal motivo, para poder lograr las garantías al más mínimo riesgo residual aceptado en operaciones navales y costeras, es muy importante aplicar los controles de la seguridad tecnológica que permitan conocer y gestionar los riesgos cibernéticos a los que puedan estar sometidos las operaciones marítimas.

Por lo que el presente artículo, tiene como objetivo analizar las diferentes metodologías existentes para el tratamiento de los riesgos cibernéticos en operaciones navales y costeras, y recomendar las buenas prácticas para el diseño y adopción de un marco de referencia (framework) que se adapte a las particularidades de República Dominicana.

METODOLOGÍAS PARA LA GESTIÓN DE RIESGO EN OPERACIONES NAVALES Y COSTERAS

De acuerdo a la OMI[1] (2017), las tecnologías cibernéticas se han convertido en herramientas esenciales que permiten el funcionamiento y la gestión de los numerosos sistemas cruciales para la gestión de la seguridad y protección del transporte marítimo y del medio marino.

En ese sentido, y de acuerdo al criterio del autor de este artículo, en las operaciones navales y costeras aplican los tres (3) ejes sobre los que están basadas las metas de la ciberseguridad: i) Confidencialidad que no sean reveladas informaciones por usuarios no autorizados; ii) Integridad que no sean alterados los datos e informaciones; y la iii) Disponibilidad que los sistemas estén funcionales en todo momento.

El riesgo cibernético, según varios autores (Santos et al., 2012, Giudici, 2013; Wegener, 2013; Martín, 2015; Parada, 2018), es la probabilidad de que una amenaza explote una o varias vulnerabilidades resultando en consecuencias indeseables. Según estos mismos autores, una vulnerabilidad es una debilidad en el software / hardware, que puede ser explotada por una amenaza.

Asimismo, una amenaza es la probabilidad de que un evento explote una vulnerabilidad y provoque que sean comprometidos la confidencialidad, integridad y disponibilidad de la información.

Aunque los sistemas tecnológicos utilizados para las operaciones navales y costeras deben cumplir las normas internacionales y las establecidas como buenas prácticas de seguridad por las administraciones de abanderamiento, las vulnerabilidades generadas por el acceso, la interconexión o el establecimiento de redes entre estos sistemas, dan lugar a cualquier tipo de probabilidad de que estos sean impactados por los riesgos cibernéticos a los que están expuestos. OMI (2017) los enumera en los siguientes: a) Los sistemas del puente; b) los sistemas de manipulación de carga; c) los sistemas de propulsión y gestión de la máquina y de control de suministro eléctrico; d) los sistemas de control de acceso; e) los sistemas de servicio a los pasajeros y de organización de los mismos; f) las redes públicas para los pasajeros; g) los sistemas administra-

[1]Organización Marítima Internacional.

tivos y de bienestar de la tripulación; y h) los sistemas de comunicación (pp. 1-2).

Para establecer las buenas prácticas que permitan gestionar los riesgos cibernéticos asociados a los sistemas tecnológicos utilizados en operaciones navales y costeras, es necesario analizar las metodologías existentes, y cómo abordan cada una de estas, la gestión de los riesgos marítimos.

METODOLOGÍAS PARA LA GESTIÓN DEL RIESGO CIBERNÉTICO EN OPERACIONES NAVALES Y COSTERAS

Como órgano rector de las operaciones marítimas internacionales, se analizarán a primera instancia las directrices sobre la gestión de los riesgos cibernéticos marítimos de la Organización Marítima Internacional (OMI), a partir de las cuales se deberán sustentar las buenas prácticas para gestionar los riesgos cibernéticos marítimos.

Directriz sobre la gestión de los riesgos cibernéticos marítimos de la Organización Marítima Internacional (OMI)

De acuerdo a la OMI (2017), sus directrices presentan cinco (5) elementos funcionales que tributan al objetivo de gestionar de manera efectiva los riesgos cibernéticos.

La OMI define los elementos de la siguiente manera:

> a. Identificación. Donde se definen las funciones y responsabilidades del personal en la gestión del riesgo cibernético, se identifican los sistemas, activos, datos y otras capacidades tecnológicas, que de ser interrumpida su funcionamiento, generarán un riesgo para las operaciones de los buques.
> b. Proteger. Es donde se implementan los procedimientos y medidas para el control de los riesgos, al igual que la planificación de los planes de contingencias, con la finalidad de proteger los activos ante cualquier evento que signifique la posibilidad de ocurrencia de un riesgo cibernético y garantizar la continuidad de las operaciones del transporte marítimo.
> c. Detectar. Se crean las actividades necesarias para detectar cualquier suceso cibernético de manera oportuna.
> d. *Responder*. Donde se crean e implementan actividades y planes para dar resiliencia y restaurar los sistemas necesarios para las operaciones o servicios del transporte marítimo que hayan sido afectados por cualquier tipo de suceso cibernético.
> e. Recuperar. Es donde se determinan las medidas para copiar y restaurar sistemas cibernéticos necesarios para las operaciones de transporte marítimo que hayan sido sujeto de un suceso cibernético. (2017, p.4).

Sin embargo, de acuerdo al criterio del autor de este artículo, las directrices fundamentadas por OMI (2017) son elementos insuficientes para lograr implementar un Sistema de Gestión de Seguridad de la Información (SGSI) que vincule los cinco (5) elementos funcionales definidos. Es por tal razón, que la OMI, señala normas adicionales que tributan a las mejores prácticas para implementar la gestión de los riesgos cibernéticos, como una referencia de información más detallada a los usuarios de sus directrices.

De acuerdo a OMI (2017, p. 5), estas normas son:

> a. Directrices sobre ciberseguridad a bordo de los buques elaboradas y apoyadas por BIMCO, CLIA, ICS, INTERCARGO e INTERTANKO (mejor conocidas como normas BIMCO de ciberseguridad).
>
> b. Normas ISO / IEC 27001: Gestión de la Seguridad de la Información. Publicada por la Organización Internacional de Normalización (ISO por sus siglas en inglés).
>
> c. Marco de mejora de la ciberseguridad de las infraestructuras críticas del Instituto Nacional de Normas y Tecnologías (NIST por sus siglas en inglés) de los Estados Unidos. (2017, p. 5).

El autor de este artículo es de opinión que, independientemente se hiciera referencia a la norma ISO 27001 sobre la implementación de un SGSI, también debió hacerse referencia a la norma ISO 27005 sobre Gestión de Riesgos en la directiva de la OMI, debido a que esta es la guía que tiene las recomendaciones de cómo gestionar los riesgos de seguridad de la información que pudieran comprometer a las organizaciones, para el caso de este artículo, las operaciones marítimas.

Otro aspecto que observa el autor de este artículo, es que la directiva sobre la gestión de riesgos cibernéticos marítimos de la OMI, su alcance es concerniente a la seguridad cibernética en los buques.

Sin embargo, en las operaciones navales y costeras, existen otros elementos que integran tecnología cibernética, como por ejemplo los sensores que utilizan las boyas, entre otros, que pudieran afectar las operaciones navales y costeras, de no tomarse en consideración el salvaguardar estas tecnologías de cualquier incidente cibernético que ponga en riesgo el buen funcionamiento de los mismos.

Directrices sobre ciberseguridad a bordo de los buques elaboradas y apoyadas por BIMCO[2], CLIA, ICS, INTERCARGO e INTERTANKO (Guía BIMCO)

La guía BIMCO, de acuerdo a Erawat (2016), es el primer enfoque sistemático para la gestión de riesgos de ciberseguridad en buques. Esta directiva está compuesta por un enfoque para la gestión del riesgo establecido en seis (6) procesos, que de acuerdo a BIMCO (2018), son:

a. Identificación de las amenazas, donde se deben comprender las amenazas cibernéticas externas al buque.

b. Identificar las vulnerabilidades, proceso en el cual se realizan los inventarios de los sistemas a bordo del buque, con enlaces de conexión directa e indirecta a redes de comunicación.

c. Evaluación de la exposición al riesgo, donde se determina la probabilidad de que una vulnerabilidad sea explotada por amenazas externas.

d. Desarrollar medidas de protección y detección, lo que permite reducir la probabilidad de que las vulnerabilidades sean explotadas, y esto permite reducir el impacto en caso contrario.

e. Establecer planes de contingencia, en donde se diseña y prioriza los planes de contingencias para mitigar cualquier riesgo cibernético potencial identificado.

f. Responder y recuperarse de un incidente de ciberseguridad, este proceso se logra utilizando las buenas prácticas definidas en los planes de contingencia.

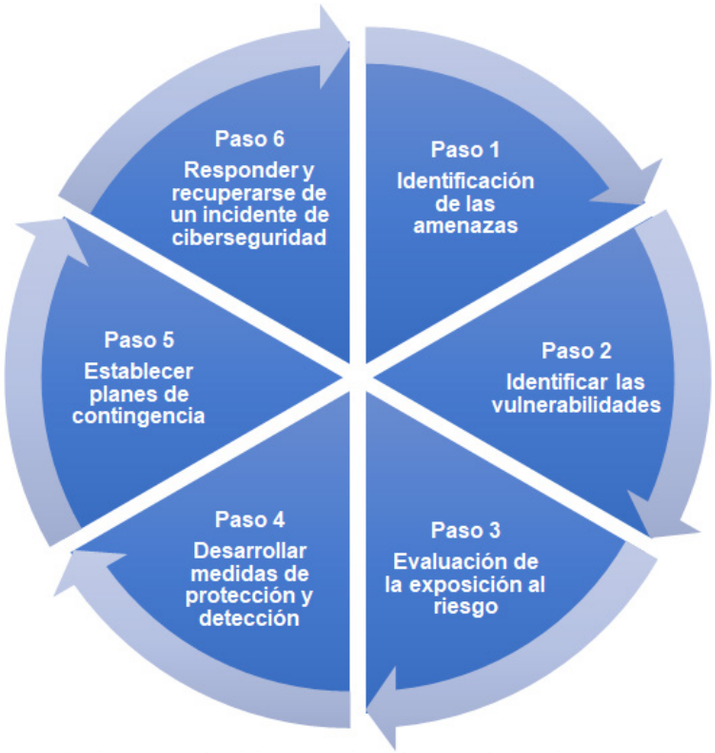

Figura 1. Enfoque gestión del riesgo cibernético según las directrices BIMCO. Fuente: Recreado de Guías BIMCO (2018, p. 4).

Asimismo, el autor de este artículo es del criterio de que la guía BIMCO ofrece un listado más detallado que el definido por la directiva de la OMI (2017) de los sistemas, equipos y tecnologías a bordo de un buque que pueden ser objeto de ataques cibernéticos. Estos quedan agrupados en el mismo contexto de categorías establecidos por la directiva OMI.

Sistema de Gestión de Seguridad de la Información – Normas ISO / IEC 27001

Es del criterio del autor de este artículo, que las normas ISO / IEC 27001 son un estándar mundial de buenas prácticas para establecer un sistema de gestión de la seguridad de la información, y por tanto, aunque estas no están directamente orientadas al sector marítimo, su metodología puede ser utilizada para ser aplicada en la gestión de riesgos cibernéticos en operaciones navales y costeras, acompañado del estándar ISO / IEC 27005 de las mismas normas, pero orientado a la gestión de riesgos.

[2]Consejo Marítimo Internacional del Báltico (BIMCO por sus siglas en inglés).

En ese mismo sentido opina Erawat (2016), cuando señala que las normas ISO 27000 son un estándar aplicable a todo tipo de organizaciones y que son guías reconocidas en el ámbito de la ciberseguridad.

De acuerdo al ISO 27000 (2018), este estándar está compuesto por las siguientes publicaciones principales que conforman un SGSI:

a. ISO / IEC 27001, es la certificación que deben de obtener las organizaciones y que contiene las especificaciones para la implementación de un SGSI.

b. ISO / IEC 27002, es la norma que contiene las buenas prácticas para la gestión de la seguridad de la información.

c. ISO / IEC 27003, esta norma es el soporte de la ISO / IEC 27001, ya que contiene las directrices para la implementación de un SGSI.

d. ISO / IEC 27004, establece las métricas para la gestión de la seguridad de la información.
e. ISO / IEC 27005, contiene las buenas prácticas sobre la gestión de riesgos para la seguridad de la información.

Marco de mejora de la ciberseguridad de las infraestructuras críticas del Instituto Nacional de Normas y Tecnologías de los Estados Unidos (NIST Cybersecurity Framework CSF)

De acuerdo a Erawat (2016), la guía NIST se publicó en el año 2014 por el Instituto Nacional de Estándares y Tecnologías de Estados Unidos y es de libre consulta y aplicación. De acuerdo al criterio de este autor, esta guía posee un enfoque bastante adecuado para gestionar la ciberseguridad en infraestructuras críticas, por lo que considera, puede ser adoptado en el sector del transporte marítimo.

En ese mismo sentido, Erawat señala que los cinco elementos que presenta la OMI (2017, p. 4) en su directiva, son los mismos indicados por la guía NIST CSF.

Función	Identificador función	Identificador categoría y descripción
ID	Identificar	ID.AM Gestión de activos
		ID.BE Entorno del negcoio
		ID.GV Gobierno
		ID.RA Análisis de riesgos
		ID.RM Estrategia gestión de riesgos
PR	Proteger	PR.AC Control de accesos
		PR.AT Concienciación y formación
		PR.DS Seguridad de datos
		PR.IP Procesos y procedimientos para protección de información
		PR.MA Mantenimiento
		PR.PT Tecnologías de protección
DE	Detectar	DE.AE Anomalías y eventos
		DE.CM Monitorización continua de la seguridad
		DE.DP Procesos de detección
RS	Responder	RS.RP Planificación de la respuesta
		RS.CO Comunicaciones
		RS.AN Analisis
		RS.MI Mitigación
		RS.IM Mejoras
RC	Recuperar	RC.RP Planificación de la recuperación
		RC.IM Mejoras
		RC.CO Comunicaciones

Figura 2. Funciones y categorías del Marco de Referencia NIST CSF. Fuente: Recuperado de Erawat (2016).

De acuerdo a la Figura 2 se puede visualizar que, dentro de este marco de referencia diseñado por la NIST, se pueden encontrar para cada uno de los cinco elementos funcionales de la guía OMI, las categorías y subcategorías de los controles de ciberseguridad que pueden ser utilizados para aplicar a cada elemento funcional, y cuyos controles están identificados por un código como se muestra en la figura indicada.

CONCLUSIÓN

Visto lo analizado en el presente artículo, el autor concluye con lo siguiente:

a. Con la publicación de la directiva sobre la gestión de riesgos cibernéticos marítimos de la OMI, queda claramente evidenciado el criterio del autor de este artículo, respecto a que las

operaciones navales y costeras no escapan a los ataques de la guerra cibernética.

b. Es necesario diseñar e implementar, sustentado en las directrices / marcos de referencias establecidos por la OMI y analizadas sus principales características en este artículo, un Sistema de Gestión de Seguridad de la Información (SGSI) que se adapte a las particularidades de las Operaciones Navales y Costeras de República Dominicana, y que permita dar respuesta efectiva a la gestión de riesgos cibernéticos en este sector.

c. Se deberá considerar, el diseño del SGSI a proponer, como un estándar militar que vincule las dependencias del Ministerio de Defensa que deben salvaguardar la soberanía nacional en actividades relacionadas a las operaciones navales y costeras.

d. El diseño del SGSI a proponer, deberá de considerar la gestión de riesgos cibernéticos en todo lo que se relaciona con las operaciones navales y costeras, y no solo enfocado a la protección de la tecnología en buques, como lo establecen las directivas de la OMI y la guía BIMCO.

REFERENCIAS

BIMCO. (2018). *Directrices sobre la seguridad cibernética a bordo de buques.* Recuperado de https://www.bimco.org/-/media/bimco/about-us-and-our-members/publications/ebooks/cyber-security-guidelines-2018.ashx

Erawat. (2016). *Guía OMI ciber riesgo y buenas prácticas ciberseguridad* [Mensaje en un blog]. Recuperado de http://erawat.es/es/guia-omi-ciber-riesgo

Giudici, D. E. (2013). *Lineamientos para la seguridad cibernética en Teatro de Operaciones.* Recuperado de http://190.12.101.91:80/jspui/handle/123456789/176

Martín, P. E. (2015). Inseguridad cibernética en América Latina: Líneas de reflexión para la evaluación de riesgos. *Instituto Español de Estudios Estratégicos, 8.* Recuperado de http://www.ieee.es/

Organización Marítima Internacional. (2017). *Directrices sobre la gestión de los riesgos cibernéticos marítimos.* Recuperado de http://www.imo.org/es/ourwork/security/guide_to_maritime_security/paginas/cyber-security.aspx

Parada, D. J., Flórez, A., y Gómez, U. E. (2018). Análisis de los componentes de la seguridad desde una perspectiva sistémica de la dinámica de sistemas. *Información Tecnológica, 29*(1), 27-38. doi: dx.doi.org/10.4067/S0718-07642018000100027

Santos-Olmo, L. A., Fernández-Medina, E., y Piattini, M. (2012). *Revisión sistemática de metodologías y modelos para el análisis y gestión de riesgos asociativos y jerárquicos para PYMES.* Recuperado de https://www.researchgate.net

Wegener, H. (2013). Los riesgos económicos de la ciberguerra. *Cuadernos de Estrategia, 162, 177-227.* Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=4276097