




REVISTA DERROTERO

Seguridad y Defensa

Ciberseguridad y ciberdefensa para la Armada Nacional

Juan Andrés Suarez Acuña ¹ y Juan Felipe Morantes González ²

¹Ingeniero electrónico. Coordinador interinstitucional Armada de Colombia. Unidad ARC, Dirección Contra las Drogas, Bogotá, Colombia.

²Profesional en ciencia navales. Unidad ARC, Dirección Contra las Drogas, Cartagena, Colombia.



Recibido: 26/05/2021

Aprobado: 18/09/2021

Correspondencia:

juan.suarez
@armada.mil.co

juan.morantes
@armada.mil.co

Citación:

J. Suarez-Acuña y J. Morantes-González.
Ciberseguridad y ciberdefensa para la Armada Nacional. Derrotero 15, número 1 (Ene-Dic) 2021.

Resumen

Al tener en cuenta la dependencia tecnológica que apoya los procesos y los procedimientos al interior de la Armada Nacional para la acertada toma de decisiones, es importante contar con: estrategias de ciberseguridad orientadas a la protección de la infraestructura tecnológica, reducción de materialización de riesgos, incorporación de estándares aprobados y recurso humano con conocimientos en cultura de ciberseguridad, ya que así se abordan las diferentes amenazas cibernéticas, impactando de forma directa o indirecta la confidencialidad, la disponibilidad de información de defensa y la seguridad nacional.

Por ello, el presente documento pretende valorar analíticamente el tratamiento de las diferentes estrategias de ciberseguridad en diferentes ámbitos, con el fin de evaluar lo más importante para incorporarlo dentro de la institución y así aportar un pensamiento crítico hacia la seguridad digital del país, como también potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades de terrorismo y delincuencia en el ciberespacio.

De esta manera se obtiene una visión global y estratégica que permite justificar la intención de contar con una dependencia al interior de la Armada Nacional para ejercer la gobernanza y armonizar, articular y guiar las responsabilidades frente a las amenazas, con el propósito de minimizar el riesgo y la afectación que estas puedan ocasionar a la prosperidad económica y social del país, y a la seguridad y defensa nacional.

Palabras clave: ciberseguridad, ciberdefensa, globalización, información, estrategia.



Cybersecurity and cyber defense for the National Navy

Abstract

Given the technological dependence that supports the processes and procedures within the Colombian Navy for correct decision-making processes, it is important to have cybersecurity strategies aimed at the protection of technological infrastructure, reduction of risk materialization, incorporation of standards approved and human resources with knowledge in cybersecurity culture. This way, different cyber threats are addressed, directly or indirectly impacting confidentiality, availability of defense information and national security. This document aims to verify the management of the different cybersecurity strategies in different national and international spheres to evaluate the key aspects to be incorporated within the institution and thus contribute with critical thinking towards the digital security of the country, as well as enhance the capacities of prevention, detection, reaction, analysis, recovery, response, investigation, and coordination in the face of terrorism and crime activities in cyberspace.

In this way a global and strategic vision is obtained that allows to justify the intention of having a dependency within the National Navy to exercise governance, harmonize, articulate and guide responsibilities in the face of threats, with the purpose of minimizing risk and effect these may cause to the economic and social prosperity of the country, and to national security and defense.

Keywords: Cybersecurity, Cyberdefense, Globalization, Information, Strategy.

Introducción

El presente documento proporciona un derrotero para el manejo de posibles estrategias y criterios que deben establecerse para controlar las amenazas cibernéticas que afectan a la Armada Nacional, ello lo hace al mencionar algunas de las amenazas que se pueden materializar, y con las acciones de promover la implementación de controles y mecanismos, y ejecutar procedimientos de inteligencia en el manejo de las ciberamenazas desde el punto de vista estratégico, operacional, táctico y técnico.

Este trabajo se basa en el método analítico bajo el enfoque teórico de Jaqueline Hurtado de Barrera y descrito en su libro “Metodología de la investigación” (?), mediante el desglose de cada uno de los elementos necesarios para orquestar las técnicas de investigación enfocadas a establecer los criterios y las estrategias que ayuden a identificar las mejores prácticas a implementar en la Armada Nacional, para obtener unos criterios de ciberseguridad y ciberdefensa que permitirían proyectar un progreso para Colombia.

Reflexión

Las amenazas cibernéticas exigen de un planteamiento que conlleve a la prevención, la detección y la respuesta, anidado a un proceso de inteligencia de amenazas, esto es debido al

carácter dinámico y cambiante de estas y que obliga a la constante actualización y revisión de los sistemas de seguridad (Martín, 2015).

Se debe tener en cuenta que las amenazas afectan a todos: los Estados, las empresas y los usuarios, por ello, compartir información y analizarla de forma eficiente puede ayudar a mejorar el nivel de seguridad, ya que los esfuerzos se diversifican entre diferentes agentes y esto requiere de una mayor colaboración entre tres tipos de agentes principales:

1. Los cuerpos y las fuerzas de seguridad de los Estados.
2. Las entidades y las empresas del mundo de la ciberseguridad.
3. Las empresas de la sociedad civil.

Es así como la colaboración interagencial mejora el conocimiento y la información, y permite dotar de mayor inteligencia a los sistemas de ciberseguridad. Todo ello requiere de una diversificación y ampliación de las fuentes de información sobre las amenazas y su análisis de forma conjunta, es decir, es necesario compartir información y que esta sea compatible para ser analizada, ya que el desarrollo de sistemas inteligentes, basados en el análisis de información (González, 2007), y la búsqueda de correlaciones son la respuesta a la necesidad de desarrollar políticas proactivas que busquen entender una amenaza antes de que un atacante pueda causar daño.

En este tema y gracias al acceso a una gran cantidad de datos consolidados, es posible distinguir potenciales amenazas, las cuales pueden ser priorizadas, ya que son capaces de correlacionar estos datos con otro tipo de información, como por ejemplo las vulnerabilidades del sistema. Esto, como ya se ha mencionado anteriormente, requiere de una monitorización constante del comportamiento de la red para que la actividad inusual pueda distinguirse del comportamiento normal.

Es así como nace la importancia de concientizar a todo el personal de la Armada Nacional, con el fin de cerrar las brechas ante los peligros de la era actual en temas de procesos relacionados con la ciberseguridad y la ciberdefensa, por tal razón es necesario desglosar e informar cada una de las fases que se deben implementar en nuestras organizaciones, las cuales son prevención, detección y respuesta y se describen a continuación:

A. Prevención

Dentro de las etapas que se plantean en la gestión de la información, la prevención es uno de los puntos álgidos a ser tenidos en cuenta, ya que por un lado están los activos críticos de la organización y por otro se encuentra el usuario final, el cual es responsable de mantener esas políticas impuestas por un oficial de seguridad de la información. Por esto, es trascendental conocer el progreso de las amenazas, de las posibles estafas y de qué



Figura 1. Etapas en la gestión de la ciberseguridad

Fuente: (Fundación Telefónica, 2016).

soluciones existen contra ellas: la formación constante es un elemento esencial en la prevención (Vásquez y Cárdenas, 2015).

Se debe pensar que incluso se pueden ver afectados nuestros activos informáticos si no se activan las debidas protecciones a las instalaciones físicas, ya que es común encontrar en las organizaciones personal no autorizado ingresando a los Centros de Operaciones de Seguridad (SOC) y también al Centro de Operaciones de Redes (NOC), por tal motivo se debe invertir en mecanismos que logren efectuar un control activo del personal que efectúe cualquier tipo de cambio, por ejemplo:

i. Control de acceso y gestión de identidades

Dos procesos importantes para la ciberseguridad en una organización son el control de los accesos y la gestión de identidades. Estos dos conceptos, aunque diferentes, se dan la mano el uno con el otro para desarrollar sus funciones, las cuales son básicamente controlar los accesos a los sistemas, tanto físicos como informáticos. En palabras de (Garzón, 2017) sería:

La gestión de identidades es un proceso relevante a la hora de prevenir ataques, ya que consiste en asignar a una identidad concreta un rol o una serie de permisos o credenciales para acceder a ciertos sistemas o recursos, especialmente a las aplicaciones críticas y zonas restringidas. En todas las organizaciones existen zonas donde se almacena información confidencial o de suma importancia. Por eso es recomendable implementar una serie de políticas de control sobre quiénes podrán acceder a los

activos críticos para minimizar el riesgo, y esto se realiza mediante las herramientas que nos ofrecen el control de accesos y la gestión de identidades (2017).

Al pensar en la correcta gestión de los controles y las identidades, es necesario llevar a cabo acciones de inventariado y catalogado y establecer los criterios de acceso, los cuales deben regirse por la máxima de que una persona debe tener disponibilidad de las aplicaciones críticas o zonas restringidas solo cuando el ejercicio de su trabajo lo requiera.

Aunque en numerosas ocasiones, la gestión de identidades y el control de accesos son llevados a cabo mediante procedimientos manuales; sin embargo, los expertos en el ámbito de la gestión de identidades advierten que uno de los principales problemas que acarrea los procesos manuales en este ámbito es su ineficacia. Adicional a ello, los principales retos que la gestión de identidades plantea a las organizaciones son: la previsión, la gestión de cuentas huérfanas y la adaptación a la normativa vigente.

ii. Prevención de fugas de datos

La fuga de datos es uno de los principales problemas de seguridad y uno de los retos a los que se enfrentan usuarios, empresas y organizaciones. Los incidentes de este tipo son complejos debido a la diversidad y a las graves consecuencias que pueden acarrear. Muchas de las fugas de datos tienen un componente humano y organizativo.

Para afrontar este reto, las empresas cuentan con una amplia oferta de herramientas y medidas que de una forma eficaz ayudan a minimizar y prevenir la temida fuga de datos, y estas se pueden agrupar en tres grupos diferentes: en el primero se englobarían todas las medidas técnicas, en el segundo estarían las de carácter organizativo y en el tercero las medidas legales.

Entre las medidas técnicas se hallan: control de acceso e identidad, soluciones anti-malware y antifraude, seguridad perimetral y protección de las comunicaciones, control de contenidos y de tráfico, copias de seguridad, control de acceso a los recursos, actualizaciones de seguridad y parches y, por último, otras medidas de seguridad derivadas del cumplimiento de legislación, gestión de eventos e inteligencia de seguridad.

En cuanto al ámbito organizativo, las actuaciones que se pueden desarrollar son: establecer un código de buenas prácticas, una política de seguridad, unos procedimientos de clasificación de la información, el establecimiento de roles y niveles de acceso, la formación e información interna y sistemas de gestión de seguridad de la información (Zuleta, 2015).

iii. Seguridad de red

La seguridad de red hace referencia a todas aquellas acciones encaminadas y diseñadas

para proteger una red de sistemas u ordenadores y recursos de acceso de red. Esencialmente, estas actividades se encaminan a proteger el uso de las redes, el grado de fiabilidad, la integridad y su seguridad y la de los datos que se transmiten a través de ellas. Su efectividad va enfocada en la protección de una amplia variedad de amenazas y busca evitar su entrada en la red o que se expanda por ella, por lo que es un elemento esencial de una correcta política de prevención en materia de ciberseguridad (Guglieri, 1996).

De acuerdo con esta idea, para proteger nuestra red de virus, troyanos, espías, *hackers*, robos de identidades, etc., es necesario contar con varias capas de seguridad para que si una falla, la otra actúe y detenga la amenaza. En este sentido, se refiere a una estructura en forma de anillos o capas, similar al concepto que ya se ha comentado sobre los sistemas operativos de confianza.

En cuanto a la seguridad de la red, será necesario implementar medidas de seguridad tanto de *hardware* como de *software*. Este último, además, requerirá de una actualización constante, lo que reducirá las posibilidades de ser afectado por una amenaza.

Así, los principales componentes que normalmente incluye esta política de seguridad en el apartado del *software* son el antivirus, el antispyware y los cortafuegos con los que se bloquean accesos no autorizados a la red. Existen además sistemas que analizan constantemente datos sobre el uso de las redes y que pueden ayudar a descubrir intrusos a través de la detección de anomalías en estos usos. En referencia al hardware, las medidas suelen estar encaminadas al control de acceso mediante sistemas de autenticación, como por ejemplo los de tipo biométrico o los token de seguridad (Enrique, 2014).

En resumen, una política de seguridad de la red debe incluir tres pasos fundamentales: la definición clara sobre nuestra red, su implementación y su continua auditoría.

B. Detección

En el campo de la ciberseguridad, otro proceso destacado es la detección de incidencias. Esta puede ocurrir mientras se está produciendo el ataque o pasado un tiempo desde el mismo, ya que la detección de un ataque o una amenaza en tiempo real suele producirse gracias a la detección del *malware* por parte de un antivirus. Si por el contrario se da la segunda circunstancia, los problemas son mayores porque los *hackers* han podido actuar libremente durante un largo periodo de tiempo. Se estima que el promedio entre el momento en que se produce una brecha de seguridad y su detección fue (en 2014) de 205 días (Pérez, 2012).

Afortunadamente, se puede afirmar que las herramientas de ciberseguridad existentes en la actualidad realizan de forma eficaz la detección de patrones de ataque conocidos si se

encuentran instaladas correctamente. El problema lo encontramos con los ataques con patrones desconocidos y cuando la detección no se ha producido en tiempo real y ha pasado un periodo largo hasta que finalmente se produce la detección. Esto se ha convertido en un problema creciente porque la forma de actuar de los *hackers* ha cambiado notablemente en los últimos años, se ha pasado de un modelo de ataques con patrones más reconocibles, en momentos concretos y determinados, a un modelo de ataques diversificados que se pueden producir en cualquier momento (Newmeyer, Cubeiro y Sánchez, 2015) y según las reflexiones de Monsalve Méndez y de González y Montenisio:

La gestión de vulnerabilidades y la monitorización son ahora los dos grandes procedimientos que se ejecutan para interponer una barrera a la detección de las amenazas (Monsalve, 2018).

Ambos son fundamentales para una correcta detección, los dos procedimientos se apoyan el uno al otro. Así, dentro del plan de gestión de vulnerabilidades es necesario contemplar una monitorización continua de los sistemas informáticos de la empresa u organización. La gestión de vulnerabilidades permite obtener una visión continua de las flaquezas y debilidades en el entorno de las TI y de los riesgos que se le asocian. Solamente identificándolos y mitigándolos, una organización puede prevenir los ataques que pretendan penetrar en las redes de una empresa u organización y robar información.

Es importante no confundir la gestión de vulnerabilidades con el escaneo de vulnerabilidades. Las dos se encuentran relacionadas, pero la segunda consiste en la utilización de un programa informático con el que se identifican los puntos débiles de nuestra red, la infraestructura informática o las aplicaciones. La primera es el proceso que engloba la búsqueda de estos puntos débiles y que tiene en cuenta otros aspectos como los riesgos que pueden ser aceptados o las soluciones que van a requerir un riesgo determinado. Por ello, su objetivo principal es detectar y solucionar las debilidades de manera oportuna (2018).

C. Respuesta

Si desafortunadamente se ha producido un ataque y los equipos o sistemas se han visto infectados, es importante actuar en varios campos. Por un lado, dar una respuesta técnica y, si finalmente se ha producido un robo de identidad o robo de datos, acudir a las fuerzas y cuerpos de seguridad del Estado e iniciar acciones legales para que los delitos que se hayan podido cometer no queden impunes (Lessig, 2002).

Para dar una respuesta técnica es primordial seguir cinco pasos con los que se podrá prevenir un robo de datos o acortar el impacto negativo del ataque:

En primer lugar, hay que desconectar el equipo de internet. Con la desconexión se podrá impedir que el virus que infectó el equipo continúe propagándose por la red y que se produzca una nueva infección después de la limpieza.

En segundo lugar, y si esto no se había realizado ya con anterioridad, instalar un programa antivirus. Como se ha comentado en el apartado anterior, es muy recomendable la utilización de herramientas proactivas mejor que reactivas, por lo que es deseable instalar un *software* que incluya capacidades de detección proactiva de amenazas. Si ya contábamos

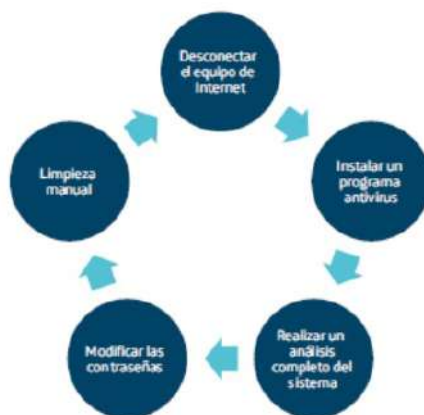


Figura 2. Pasos frente a un ciberataque

Fuente: (Fundación Telefónica, 2016).

con un antivirus, otra acción fundamental es la de descargar y actualizar su base de firmas para conseguir un análisis más eficiente del equipo (Llinares, 2013).

En tercer lugar, se debe realizar un análisis completo del sistema. Es muy importante analizar por completo todos los discos del equipo en busca de amenazas o daños.

La cuarta acción que se debe abordar es modificar todas las contraseñas de cualquier servicio que requiera de una autenticación. Con este procedimiento eliminaremos toda posibilidad de robo de credenciales por parte de los cibercriminales que se encuentran detrás del *malware*.

Por último, y en caso de resultar necesario, se debería realizar una limpieza manual, no siempre es suficiente con escanear el sistema y los procesos automatizados. Veamos tres fases de este último paso:

i. Sistemas de recuperación

Los sistemas de recuperación han sido una excelente característica que se ha implementado en los sistemas operativos para restaurar a un punto de partida anterior (uno donde se conozca que no posee ningún error), esto con el fin de corregir y solucionar los *bugs* o algún tipo de problema a nivel de Kernel.

Uno de los sistemas operativos pioneros en incluir esta función fue Microsoft en sus sistemas operativos de Windows. En la primera versión que se añadió fue en Windows ME y, a partir de entonces, se ha introducido en todas las versiones del sistema operativo que le han seguido.

En sus primeras versiones, este sistema se basaba en un filtro de archivos que observaba los cambios que sufrían las diferentes extensiones, copiando los archivos antes de ser sobrescritos. Posteriormente, en las versiones a partir de Windows Vista, se utiliza un *Shadow System* de restauración que permite cambios de bloque en archivos ubicados en cualquier directorio, de forma que reciben apoyo y son monitorizados con independencia de su ubicación; el sistema también permite realizar recuperaciones si la versión de Windows instalada no consigue limpiar el sistema.

Otro sistema operativo que ha introducido esta función ha sido Android. Aquí se llama *recovery* y se basa en una partición con propiedades de arranque, el cual se ejecuta por separado y en paralelo al sistema operativo principal de Android. En este, las particiones en que se dividen son boot/kernel y root/system, y se encuentran separadas del sistema de recuperación que contiene su propio Kernel de Linux.

ii. Evidencias digitales

Por evidencia digital se entiende cualquier documento, fichero, registro o dato contenido en un soporte informático, susceptible de tratamiento digital y que puede ser utilizado como prueba en un proceso legal (Buzai, 2012).

iii. Inteligencia

El carácter dinámico y cambiante de las amenazas cibernéticas obliga a la constante actualización y revisión de los sistemas de seguridad, lo que se traduce en que la ciberseguridad es un proceso costoso, en recursos económicos y en tiempo. Además, es de recordar que las amenazas afectan a todos: Estados y empresas (?).

Por ello, compartir información y analizarla de forma eficiente puede ayudar a mejorar el nivel de seguridad y a economizar costes, ya que los esfuerzos se diversifican entre diferentes agentes y como se había mencionado anteriormente, esto requiere de una mayor colaboración entre tres agentes principales:

- i. Los cuerpos y fuerzas de seguridad de los Estados.
- ii. Las entidades y empresas del mundo de la ciberseguridad.
- iii. Las empresas de la sociedad civil.

También recordamos que la colaboración entre agentes mejora el conocimiento y la información, y permite dotar de mayor inteligencia a los sistemas de ciberseguridad. Todo ello requiere de la diversificación y la amplitud de las fuentes de información sobre las amenazas para analizarlas de forma conjunta, es decir, es necesario compartir información y que esta sea compatible para ser analizada (Enrique, 2014).

Dado todo lo anterior, es imperativo contar con el respaldo de todas las entidades gubernamentales de Colombia, esto con el fin de concientizar sobre la importancia de la ge-

neración de talento humano en ciberseguridad y ciberdefensa, y determinar cuáles son las causas de la falta de investigación, innovación y emprendimiento en esta área, además que permitan la creación de herramientas que den respuesta a los nuevos tipos de ataques y que se genere confianza en el entorno digital.

Ahora, con el presente trabajo se proponen los siguientes objetivos y líneas de acción para fortalecer el talento humano necesario para la protección y la defensa.

Objetivo general 1: incrementar las capacidades de emprendimiento en Colombia en materia de ciberseguridad y ciberdefensa para el cuatrienio 2019-2023.

Objetivos específicos: fomentar la creatividad y la innovación en I+D+I en materia de ciberseguridad y ciberdefensa para las entidades públicas y privadas en Colombia.

Líneas de acción

1. Aumentar en un 10 % el presupuesto de inversión en materia de I+D+I en cada uno de los sectores públicos y privados.
2. Estimular con beneficios tributarios a las empresas privadas que contribuyan al fomento del I+D+I en materia de ciberseguridad y ciberdefensa.
3. Realizar gestiones con el Ministerio de Hacienda para que se asigne un mayor presupuesto para la inversión en materia de ciberseguridad y ciberdefensa.

Objetivo general 2: aumentar las competencias y los conocimientos especializados en ciberseguridad y ciberdefensa en Colombia para el periodo 2019-2023.

Objetivos específicos: desarrollar programas, proyectos y campañas de sensibilización y concientización en ciberseguridad para los sectores público y privado.

Líneas de acción

1. Potenciar la concientización del entorno digital y su problemática tanto en Colombia como a nivel mundial. Para ello se deberá diseñar e implementar un programa tendiente a fortalecer los valores y la cultura organizacional, enfocado al ambiente digital, la ciberseguridad y la ciberdefensa, para brindar herramientas a los funcionarios de las entidades y desempeñar sus labores de forma más competitiva, así como disminuir o mitigar los factores de riesgo identificados.
2. Estímulos a la innovación mediante la promoción de becas para estudios al interior y exterior del país.

3. Desarrollar una política institucional para la retención del talento humano en materia de ciberseguridad y ciberdefensa en las entidades públicas (2019- 2023).
4. Crear una agenda nacional de seguridad digital con el fin de priorizar los intereses nacionales públicos y privados.

Conclusiones

La necesidad de proteger los servicios esenciales estratégicos de un país que hoy dependen de TI o de TO dan la importancia a la existencia de unificar los conceptos de ciberseguridad y ciberdefensa, los cuales orienten todas las medidas y las actividades a corto, mediano y largo plazo y que permitan coordinar de manera eficiente los sectores estratégicos de Colombia.

Es así que debemos enfrentar un presente con una actividad criminal que ya no solo actúa en los escenarios normales: tierra, mar y aire, sino que existen grupos organizados, delincuentes individuales, actividades de espionaje militar, industrial o político, de múltiples formas que afectan nuestras infraestructuras críticas, la integridad personal y los servicios esenciales que permiten que una sociedad sea sostenible.

Nótese que las experiencias de otros países así lo han demostrado, los ataques dirigidos por Estados que por apariencias pueden verse ejecutados por grupos criminales, con fines políticos, por reto o por lucro son cada vez más frecuentes, y en la medida en que dependemos más de la tecnología y se comprometan los intereses nacionales, este tema se convierte en estratégico para la seguridad y la defensa de Colombia.

Referencias

- [Atencio, 1979] Atencio, J. (1979). *¿Qué es la geopolítica?* ↑[Ver página](#)
- [Buzai, 2012] Buzai, G. (2012). El ciberespacio desde la geografía: Nuevos espacios de vigilancia y control global. *Meridiano*, 1, 7-52. ↑[Ver página 127](#)
- [Cano, 2011] Cano, J. (2011). Ciberseguridad y ciberdefensa: Dos tendencias emergentes en un contexto global. *Sistemas (Asociación Colombiana de Ingenieros de Sistemas)*, 119, 4-7. ↑[Ver página](#)
- [Celerier, 1961] Celerier, P. (1961). *Geopolítica y geoestrategia*. ↑[Ver página](#)
- [Enrique, 2014] Enrique, S. (2014). *Seguridad y defensa del ciberespacio*. Editorial Dunker. ↑[Ver página 124](#), [127](#)

- [Fundación Telefónica, 2016] Fundación Telefónica. (2016). *Ciberseguridad, la protección de la información en un mundo digital*. Madrid, España: Fundación Telefónica. ↑Ver página 122, 126
- [Garzón, 2017] Garzón, M. (2017). *Diseñar los controles de acceso aplicables a la empresa Spytech SAS para su posterior implementación, de acuerdo con el dominio A9 de la norma ISO 27001: 2013* (tesis de especialización). Universidad Nacional Abierta y a Distancia, Bogotá, Colombia. ↑Ver página 122
- [González y Montesino, 2018] González, H. y Montesino, R. (2018). Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones web. *Revista Cubana de Ciencias Informáticas*, 12(4), 52-65. ↑Ver página
- [González, 2007] González, I. (2007). Cibernética y sociedad de la información: El retorno de un sueño eterno. *Signo y Pensamiento*, 26(50), 84-99. ↑Ver página 121
- [Guglieri, 1996] Guglieri, J. (1996). *Reingeniería y seguridad en el ciberespacio*. Madrid, España: Ediciones Díaz de Santos. ↑Ver página 124
- [Lessig, 2002] Lessig, L. (2002). Las leyes del ciberespacio. *THĒMIS-Revista de Derecho*, 44, 171-179. ↑Ver página 125
- [Llinares, 2013] Llinares, F. (2013). La respuesta penal al ciberfraude: Especial atención a la responsabilidad de los muleros del phishing. *Revista Electrónica de Ciencia Penal y Criminología*, 15(12). ↑Ver página 126
- [Martín, 2015] Martín, P. (2015). *Inseguridad cibernética en América Latina: Líneas de reflexión para la evaluación de riesgos*. Recuperado de https://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEE079-2015_InseguridadCibernetica_AmericaLatina_PaulE.Martin.pdf ↑Ver página 121
- [Monsalve, 2018] Monsalve, J. (2018). *Ciberseguridad: Principales amenazas en Colombia (ingeniería social, Phishing y Dos)* (tesis). Universidad Piloto de Colombia, Bogotá, Colombia. ↑Ver página 125
- [Newmeyer, Cubeiro y Sánchez, 2015] Newmeyer, K., Cubeiro, E. y Sánchez, M. (2015). *Ciberespacio, ciberseguridad y ciberguerra. Ponencia presentada en el II Simposio Internacional de Seguridad y Defensa*, Lima, Perú ↑Ver página 125
- [Pérez, 2012] Pérez, M. (2012). Tecnologías para la defensa en el ciberespacio. En Ministerio de Defensa, *El ciberespacio: Nuevo escenario de confrontación* (pp. 253-306). Madrid, España: Ministerio de Defensa. ↑Ver página 124

- [Pérez, J. y Ramos, 2003] Pérez, J. y Ramos, I. (2003). La inteligencia, la memoria social y el ciberespacio. *Revista Novatica*, 165, 18. ↑[Ver página](#)
- [Romero, 2011] Romero, J. (2011). Estrategias nacionales de ciberseguridad: Ciberterrorismo. *Cuadernos de Estrategia*, 149, 257-322. ↑[Ver página](#)
- [Rustici, 2012] Rustici, R. (2012). Armas cibernéticas: La igualdad de condiciones a nivel internacional. *Military Review*, 25. ↑[Ver página](#)
- [Vásquez y Cárdenas, 2015] Vásquez, K. y Cárdenas, M. (2015). *Propuesta de buenas prácticas para fortalecer los controles de prevención y detección temprana del cibercrimen en las empresas colombianas* (tesis). Pontificia Universidad Javeriana, Bogotá, Colombia. ↑[Ver página 122](#)
- [Zuleta, 2015] Zuleta, S. (2015). *Protección de datos personales en Colombia* (tesis). Universidad Militar Nueva Granada, Bogotá, Colombia. ↑[Ver página 123](#)