Análisis y estrategia de implementación de un marco de trabajo de ciberseguridad para la unidad de Ciberdefensa del Ejército Nacional.

Capitán Gómez C. Carlos, May S. Luciano, Franco V. Carlos
Estudiantes de Maestría en seguridad de la información
Departamento de ingeniería de sistemas y computación
Universidad de los Andes
Colombia noviembre 2020

Resumen – Este documento presenta la metodología utilizada para el análisis y estrategia de implementación de un marco de trabajo de ciberseguridad para la unidad de Ciberdefensa del Ejército Nacional. Este trabajo responde a la problemática identificada de ausencia de procesos definidos para la priorización, investigación y respuesta de incidentes cibernéticos.

En el desarrollo de este proyecto se revisó la literatura disponible sobre los marcos de Ciberseguridad más usados y se definieron los criterios de evaluación de los mismos para realizar una selección adecuada que se adapte a la Unidad de Ciberdefensa del Ejercito Nacional. Este es el primer paso para la implementación de dicho marco de Ciberseguridad.

Índice de Términos – Ciberdefensa Ciberseguridad, Framework, Ciberespacio, Fuerzas Militares, Ejército Nacional de Colombia.

I. Contexto

El artículo 217 de la Constitución Política de Colombia consagra que "La Nación tendrá para su defensa unas Fuerzas Militares permanentes constituidas por el Ejército, la Armada y la Fuerza Aérea. Las Fuerzas Militares tendrán como finalidad primordial la defensa de la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional."[1]. La misión del Ejército Nacional de Colombia es "El Ejército Nacional conduce operaciones militares orientadas a defender la soberanía, la independencia y la integridad territorial y proteger a la población civil y los recursos privados y estatales para contribuir a generar un ambiente de paz, seguridad y desarrollo, que garantice el orden constitucional de la nación."[2] ,

Teniendo en cuenta esto, es deber del Ejército Nacional garantizar la defensa de la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional en todos los dominios de guerra: "Tierra, Mar, Aire, Espacio y el denominado quinto dominio de guerra el Ciberespacio"[3]

Fig. 1. Quinto Dominio de la Guerra – Tomada de https://www.ccoc.mil.co/quienes_somos/ccoc/el_quinto_dominio_guerra

Siendo el Ciberespacio un nuevo dominio de Guerra, el Ejército Nacional de Colombia debe prepararse para incursionar en él. Este quinto dominio trae consigo varias problemáticas como el anonimato en los ataques cibernéticos, la atribución de los ataques cibernéticos y la definición de las fronteras geográficas.

El estado colombiano consciente de la complejidad del Ciberespacio y teniendo en cuenta la digitalización y la globalización mundial, donde cada día el uso de las tecnologías de la información y las comunicaciones es más necesaria para las actividades diarias en aspectos variados, conforma una estrategia de Ciberdefensa para el país, en la cual el Ejército Nacional debe adaptarse rápidamente a este reciente escenario de guerra con el fin de prepararse para posibles confrontaciones que intenten afectar la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional.

[1] http://wsp.presidencia.gov.co/Normativa/Documents/Constitucion-Politica-Colombia.pdf.

[2] https://www.ejercito.mil.co/conozcanos/mision_vision/mision.

[3] https://www.ccoc.mil.co/quienes_somos/ccoc/el_quinto_dominio_guerra

La Ciberdefensa en Colombia inició para la Fuerzas Militares en el año 2011 con el documento CONPES 3701 (Consejo Nacional de Política Económica y Social et al., 2011) (Consejo Nacional de Política Económica y Social CONPES), en el cual se estable la estrategia de Ciberdefensa para Colombia y su vez, se emiten los lineamientos para la política de Ciberseguridad y Ciberdefensa.

Basados en esta estrategia se creó una comisión intersectorial conformada por el ColCERT de Colombia, quien es el CERT de Colombia, el Centro cibernético Policial (CCP) y el Comando Conjunto cibernético de las Fuerzas Militares de Colombia, quienes son los encargados de liderar la Ciberdefensa y la Ciberseguridad del país.

Fig. 2. Comité Intersectorial –Tomado del CONPES 3701

El Comando Conjunto Cibernético de las Fuerzas Militares de Colombia lideró la creación de las Unidades de Ciberdefensa en cada una de las Fuerzas Militares y así, para el año 2012, se inició con la creación y montaje de la unidad de Ciberdefensa del Ejército Nacional de Colombia.

Fig. 3. Unidades del Ciberdefensa en las Fuerzas Militares – Tomado de https://www.cci-es.org/

En el año 2016 el Departamento Nacional de Planeación (DNP) emite un nuevo documento CONPES 3854 – Política Nacional de Seguridad Digital (Presidencia de la República de Colombia, 2016) (Consejo Nacional de Política Económica y Social CONPES 3854), en el cual fortalece la seguridad digital del país y continúa con la estrategita de Ciberdefensa para Colombia de acuerdo al CONPES 3701, al igual que con el documento CONPES 3995 – Política Nacional de Confianza y Seguridad Digital (Departamento Nacional de Planeación, 2020).

Ya con la Unidad de Ciberdefensa creada y teniendo en cuenta los documentos CONPES, el Ejército Nacional matricula unos proyectos ante el Departamento Nacional de Planeación (DNP) con el nombre "IMPLEMENTACIÓN UNIDAD DE CIBERDEFENSA EJERCITO y FORTALECIMIENTO DE LOS MEDIOS CIBERNÉTICOS DEL EJÉRCITO NACIONAL", con los cuales el Ejército Nacional inicia el desarrollo de la capacidad de Ciberdefensa en el Ejército Nacional.

II. Problema

En el desarrollo de la capacidad con el apoyo de tecnologías de seguridad para la protección de la infraestructura tecnológica militar, el Ejército Nacional comenzó a evidenciar los ataques cibernéticos que se reciben a diario buscando vulnerar la integridad, disponibilidad y confidencialidad de la información

La unidad de Ciberdefensa del Ejército Nacional requiere la construcción de procesos definidos para la gestión de incidentes cibernéticos con el fin de facilitar la toma de decisiones y poder tomar cursos de acción para la priorización, investigación y respuesta de los incidente detectados o reportados, así mismo generar una retroalimentación basados en bases de conocimientos y lecciones aprendidas, que faciliten la evolución de la unidad de Ciberdefensa.

III. Propuesta

Diseñar e implementar el plan para la gestión de incidentes de seguridad para la unidad de Ciberdefensa del Ejército Nacional.

Para implementar el marco se plantean las siguientes etapas de desarrollo:

- Revisar la literatura de marcos de Ciberseguridad más usados con el fin de seleccionar el que más se adapte a la unidad de ciberdefensa del Ejército Nacional.
- Definir los criterios de evaluación de los marcos de Ciberseguridad que proporcionen procedimientos y controles de seguridad apropiados para la capacidad instalada en la unidad de Ciberdefensa del Ejército Nacional.
- Seleccionar el marco de Ciberseguridad con base en los criterios definidos.

- Establecer una propuesta para la implementación de la respuesta de incidentes de un marco de Ciberseguridad para la Unidad de Ciberdefensa del Ejército Nacional.

IV. Selección del Marco

La construcción del plan para la gestión de incidentes requiere primero seleccionar un marco de ciberseguridad que permita incorporar procesos y buenas prácticas establecidas. Esta sección describe esta primera fase.

A. Arquitectura y componentes de alto nivel de la solución

Los componentes básicos que proporcionen un conjunto de actividades que lleven a lograr resultados específicos de ciberseguridad deben incluir funciones como:

- Identificar (Riesgo de ciberseguridad).
- Proteger (Asegurar la disponibilidad de servicios críticos).
- Detectar (Identificar la ocurrencia de un evento de ciberseguridad).
- Responder (tomar medidas con respecto a un incidente de ciberseguridad detectado).
- Recuperar (planes de resiliencia y restauración debido a incidentes de ciberseguridad).

Fig. 4. Tomada de - https://www.nist.gov/cyberframework

B. Definición de criterios de evaluación del marco de ciberseguridad

Esta sección presenta el conjunto de criterios que serán usados para determinar el marco idóneo para la adaptación al contexto y la implementación del mismo. Los criterios definidos procuran incluir fundamentos de ciberseguridad, incluyendo adaptabilidad de la capacidad actual, métodos para realizar tareas particulares y metodologías para la gestión de riesgos y la evaluación de sistemas y procedimientos (Consortium, 2020). También se tendrá en cuenta el tiempo de actualización de cada norma y los lineamientos que incluye en la gestión de incidentes.

1) Adaptabilidad de la capacidad instalada

Considera los lineamientos que permitan medir el nivel de madurez y la postura de seguridad de la organización (Abdullahi Garba et al., 2020) para la implementación de los procedimientos de acuerdo con las capacidades de ciberseguridad.

2) Métodos para realizar tareas en el contexto de la ciberseguridad

Considera la gestión de los diferentes tipos de datos, la protección de la infraestructura que contiene los datos y los métodos para intercambiar información con otros con el objetivo de prevenir incidentes cibernéticos en sus propias organizaciones. Cada marco establece un procedimiento o proceso que los equipos, las personas o la institución deben seguir o implementar para proteger de manera óptima los datos que poseen. Asegurarse de que esto se haga de manera coherente y fácil de completar debe garantizar que los datos permanezcan seguros (Consortium, 2020).

3) Metodologías para evaluación de la gestión

Considera las medidas de verificación en cuanto a qué tan bien se han implementado los procedimientos de ciberseguridad. Estas van desde simples verificaciones y pruebas de estrés hasta auditorías completas tanto de los sistemas físicos como de los procesos que previenen el ciberdelito por errores humanos.

4) Actualizaciones

Considera la fecha de la última actualización publicada del estándar o marco de seguridad y qué tan adaptada se encuentra al contexto actual en ciberseguridad.

5) Lineamientos en gestión de incidentes

Considera las etapas de detección y análisis de un incidente cibernético, con el fin de contenerlo, erradicarlo o recuperarlo, para salvaguardar la infraestructura tecnológica y preservar la integridad, confidencialidad y disponibilidad de la información de la institución.

C. Selección del marco de ciberseguridad

Las publicaciones del instituto NIST (*National Institute of Standards and Technology* de los Estados Unidos de América)[4], proponen grupos de controles de seguridad diferentes para ayudar a las agencias y organizaciones federales de EE. UU. a gestionar sus incidentes.

Los controles de seguridad críticos de CIS (*Critical Security Controls*) son independientes del tipo de industria y geografía y proporcionan un enfoque basado en prioridades y bastante técnico para obtener resultados inmediatos de alto impacto.

Las normas ISO 27k proponen un enfoque menos técnico y más basado en la gestión de riesgos que proporciona recomendaciones de mejores prácticas para empresas de todo tipo y tamaño (Security, n.d.)

[4] https://csrc.nist.gov/publications/sp

COBIT es un modelo que no aborda de manera completa la problemática de ciberseguridad, siendo su enfoque de gobierno de seguridad de TI, pero se ha forzado su uso por la sencillez y facilidad de su implementación (Rea-Guaman et al., 2017).

El marco de ciberseguridad del NIST se compone de un conjunto de controles y buenas prácticas de varias normas internacionales, como ISO/IEC 27001:2013, ISO/IEC 27002:2012, COBIT 5, CIS CSC, por tanto, las organizaciones pueden adaptar este marco de ciberseguridad según las necesidades y alcances que establezcan.

En el manejo de incidentes, considerado en el alcance establecido para este documento, el marco de ciberseguridad del NIST ofrecen una documentación completa, y aunque las recomendaciones están orientadas principalmente a las agencias y organizaciones federales americanas, pueden implementarse en cualquier agencia u organización de cualquier país y, como vemos en las experiencias internacionales, los países que son potencia económica lo tienen como referencia de implementación en sus estrategias de ciberseguridad.

El marco del NIST, dentro de las funciones, cuenta con guías para la etapa de preparación para la gestión de incidentes, siendo esto un punto a favor para las organizaciones porque los analistas de incidentes cuentan con las herramientas para trabajar, a diferencia de la norma ISO 27035 que no cuenta con la etapa de preparación. De igual forma el documento NIST maneja conceptos más técnicos para gestionar un incidente cibernético.

En esta evaluación también incluimos la norma NIST SP 800-61 Rev. 2 ya que ofrece una guía completa y de fácil adaptación para el proceso de gestión de incidentes que aplica al tipo de organización que nos compete y acorde con la capacidad instalada actualmente.

D. Items de cada framework seleccionado que aplican en la evaluación

1) NIST Cybersecurity Framework

ID.AM-1: Physical devices and systems within the organization are inventoried
ID.AM-2: Software platforms and applications within the organization are inventoried

PR.DS-1: Data-at-rest is protected.
PR.DS-2: Data-in-transit is protected.
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.
PR.DS-4: Adequate capacity to ensure availability is maintained.
PR.DS-5: Protections against data leaks are implemented.
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.
ID.RA-1: Asset vulnerabilities are identified and documented.
ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources.
ID.RA-3: Threats, both internal and external, are identified and documented.
ID.RA-4: Potential business impacts and likelihoods are identified.
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.
ID.RA-6: Risk responses are identified and prioritized

PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
SP 800-61 R 2 Computer Security Incident Handling

2) ISO/IEC 27001:2013 and 27002:2013

A.8.1.1 Inventory of Assets.
A.8.1.2 Ownership of Assets.
A.8.2.3 Handling of Assets.
A.8.3.1 Management of Removable Media.
A.8.3.2 Disposal of Media.
A.8.3.3 Physical Media Transfer.
A.11.2.5 Removal of Assets.
A.11.2.7 Secure Disposal or Re-Use of Equipment.
A.12.6.1 Management of Technical Vulnerabilities.
A.18.2.3 Technical Compliance Review.
A.16.1.1 Responsibilities & Procedures.
A.17.1.1 Planning Information Security Continuity.
A.17.1.2 Implementing Information Security Continuity.
A.17.1.3 Verify, Review & Evaluate Information Security Continuity

3) COBIT 5

BAI09.01 Identify and record current assets.
BAI09.02 Manage critical assets.
BAI09.03 Manage the asset life cycle.

DSS04.03 Develop and implement a business continuity
DSS05.01 Protect against malicious software.
DSS05.02 Manage network and connectivity security.
DSS06.06 Secure information assets.

APO01.06 Optimize the placement of the IT function.
APO12.01 Collect data.
APO12.02 Analyze risk.
APO12.03 Maintain a risk profile.
APO12.04 Articulate risk.
APO12.06 Respond to risk.

4) CIS Controls

Control 1.4 Maintain Detailed Asset Inventory.
Control 1,4 Maintain Detailed Asset Inventory.
Control 1,5 Maintain Asset Inventory Information.
Control 1,6 Address Unauthorized Assets.
Control 3,1 Run Automated Vulnerability Scanning Tools.

Control 19.1 Document Incident Response Procedures.
Control 19.2 Assign Job Titles and Duties for Incident Response.
Control 19.3 Designate Management Personnel to Support Incident Handling.

5) TC CYBER

ETSI GS INS 005 V1.1.1 (2011-03) Identity and access management for Networks and Services;
Requirements of an Enforcement framework
in a Distributed Environment
ETSI TS 103 523-3 Middlebox Security Protocol;
Part 3: Enterprise Transport Security.
ETSI TS 102 165-1 Methods and protocols;
Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)
GS ISI 001-1 Information Security Indicators (ISI);
Indicators (INC);
Part 1: A full set of operational indicators for organizations to use to benchmark their security posture.
GS ISI 002 Information Security Indicators (ISI);
Event Model
A security event classification model and taxonomy.
GS ISI 003 Information Security Indicators (ISI);
Key Performance Security Indicators (KPSI)
to evaluate the maturity of security event detection.
GS ISI 004 Information Security Indicators (ISI);
Guidelines for event detection implementation.
GS ISI 005 Information Security Indicators (ISI);
Guidelines for security event detection testing and assessment of detection effectiveness.

TABLA 1
Resultados de la evaluación, con base en los criterios establecidos

Criterio / Standard	Adaptabilidad de la capacidad instalada	Métodos para realizar tareas en el contexto de la ciberseguridad	Metodologías fundamentales para la gestión de riesgos	Actualizaciones	Lineamientos en gestión de incidentes
NIST Cybersecurity Framework	ID.AM-1: COBIT 5: BAI09.01, BAI09.02 ISO/IEC 27001:2013: A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4: CM-8, PM-5	PR.DS-1, PR.DS-2, PR.DS-3, PR.DS-4, PR.DS-5, PR.DS-6	Controles ID.RA-1, ID.RA-2, ID.RA-3, ID.RA-4, ID.RA-5, ID.RA-6	2018	PR.IP-9, SP 800-61 r2
ISO/IEC 27001:2013 and 27002:2013	A.8.1.1, A.8.1.2	A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7	A.12.6.1, A.18.2.3, Clause 6.1.2	2013 improvements made in 2017	A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3
COBIT 5	BAI09.01, BAI09.02	APO01.06, DSS05.02, DSS06.06, BAI09.03	APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02	2019	APO12.06, DSS04.03
CIS Controls	Control 1.4	Control 1,4 Control 1,5 Control 1,6	Control 3,1	2018	Control 19.1 Control 19.2 Control 19.3
TC CYBER	ETSI GS INS 005 V1.1.1 (2011-03)	ETSI TS 103 523-3	ETSI TS 102 165-1	2011-2017	GS ISI 001-1, GS ISI 002, GS ISI 003, GS ISI 004, GS ISI 005

La tabla presenta el resumen de los criterios usados para la selección.

Después de comparer los marcos a la luz de los criterios establecidos, se seleccionó el marco NIST descrito en el documento NIST SP 800-61 Rev. 2.

V. DESARROLLO DE LA SOLUCIÓN

A. Marco Legal

Además de las recomendaciones y guías del marco seleccionado, en el contexto de trabajo, es necesario tener en cuenta los siguientes documentos:

- CONPES 3701 - Lineamientos De Política Para Ciberseguridad Y Ciberdefensa
- CONPES 3854 - Política Nacional De Seguridad Digital
- CONPES 3995 - Política Nacional De Confianza Y Seguridad Digital
- Cybersecurity Framework – NIST
- Norma ISO/IEC 27032:2012 "Tecnologías De La Información - Técnicas De Seguridad - Directrices Para La Ciberseguridad
- NIST SP 800-61 Rev. 2 - Computer Security Incident Handling Guide

B. Metodología

La implementación del marco de ciberseguridad toma como base la norma NIST 800-61 revisión 2, donde se establece la Guía de manejo de incidentes en seguridad informática. La guía busca ayudar a las organizaciones a mitigar los riesgos de los incidentes de seguridad informática al proporcionar pautas prácticas para responder a los incidentes de manera efectiva y eficiente. También incluye pautas para establecer un programa de respuesta a incidentes efectivo, pero el enfoque principal del documento es detectar, analizar, priorizar y manejar incidentes (Cichonski, 2012).

Con base en esto, tendremos en cuenta para la realización de los procedimientos, aspectos como:

- Organización de una capacidad de respuesta a incidentes de seguridad informática.
- Manejo de un incidente
- Coordinación e intercambio de información

Además, se decidió tomar aspectos de la norma ISO/IEC 27035 que enmarca técnicas de seguridad - Gestión de incidentes de seguridad de la información. Esta norma proporciona las pautas para planificar y prepararse para la respuesta a incidentes. Las directrices se basan en la fase de "Planificación y preparación" y la fase de "Lecciones aprendidas" del modelo de "Fases de gestión de incidentes de seguridad de la información".

VI. Referencias

[1] Agence Nationale de la Sécurité des Systèmes d`Information. (2011). France ' s strategy. http://www.enisa.europa.eu/media/news-items/Information_system_security_France_strategy.pdf

[2] Baldoni, R., & Montanari, L. (2016). Italian National Cyber Security Framework. Int'l Conf. Security and Management, 16, 168–174. http://worldcomp-proceedings.com/proc/p2016/SAM9768.pdf

[3] Cichonski, P. (2012). Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology. NIST Special Publication, 800–61, 79. https://doi.org/10.6028/NIST.SP.800-61r2

[4] CIS. (2019). CIS Controls Spanish Translation. https://doi.org/ISSN 0120-5919

[5] ComplianceForge. (n.d.). Which framework is right for my business? https://www.complianceforge.com/faq/nist-800-53-vs-iso-27002-vs-nist-csf.html

[6] Consejo Nacional de Política Económica y Social, de Colombia República, & de Planeación Departamento Nacional. (2011). Lineamientos de política para ciberseguridad y ciberdefensa CONPES 3701-2011. Internet, 43.

[7] Departamento Nacional de Planeación. (2020). Politica Nacional de Confianza y Seguridad Digital. Documento CONPES 3995, 51.

[8] GOV.UK. (2018). The Minimum Cyber Security Standard. June, 1–7. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/719067/25062018_Minimum_Cyber_Security_Standard_gov.uk__3_.pdf

[9] Haviluddin, H., Mulawarman, U., & Anthony, P. (2012). COBIT Framework for Information Technology Governance (ITG) at Mulawarman University , Samarinda , East Kalimantan , Indonesia : A Descriptive Study 2012 - BIMP-EAGA CONFERENCE : " Enhancing Sustainability , Competitiveness & Innovation ". BIMP-EAGA CONFERENCE: "Enhancing Sustainability, Competitiveness & Innovation, July. https://doi.org/10.13140/2.1.4927.1365

[10] Katsikas, S., Cuppens, F., Cuppens, N., Lambrinoudakis, C., Kalloniatis, C., Mylopoulos, J., Antón, A., Gritzalis, S., Pallas, F., Pohle, J., Sasse, A., Meng, W., Furnell, S., Eds, J. G., & Goos, G. (2020). Computer Security ESORICS 2019 International Workshops - From ISO/IEC 27002:2013 Information Security Controls to Personal Data Protection Controls. February, 238–257. https://doi.org/10.1007/978-3-030-42048-2

[11] Neira, A. L., & Spohr, J. R. (2010). Sistema de Gestión de la Seguridad de la Información. Www.Iso27000.Es, 1, 14.

[12] OEA. (2019). Ciberseguridad marco nist. Http://Www.Oas.Org/Es/. http://worldcomp-proceedings.com/proc/p2016/SAM9768.pdf

[13] Osterhage, W., & Osterhage, W. (2018). Security Policy. In Wireless Network Security (Issue May, pp. 147–158). https://doi.org/10.1201/9781315106373-8

[14] Presidencia de la República de Colombia. (2016). Consejo Nacional De Política Económica Y Social Conpes. Política Nacional De Seguridad Digital, 91.

[15] Rea-Guaman, A. M., Sanchez-Garcia, I. D., Feliu, T. S., & Calvo-Manzano, J. A. (2017). Modelos de Madurez en Ciberseguridad: una revisión sistemática. Iberian Conference on Information Systems and Technologies, CISTI, June. https://doi.org/10.23919/CISTI.2017.7975865

[16] Security, H. S. (n.d.). NIST, CIS/SANS 20, ISO 27001 – Simplifying Security Control Assessments. https://www.hitachi-systems-security.com/blog/nist-cissans-20-iso-27001-simplifying-security-control-assessments/

[17] Stewart, J. M. (2016). Cybersecurity Frameworks to Consider for Organization-wide Integration. 1–9. www.globalknowledge.com

[18] The National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity. 55. https://doi.org/10.1109/isit.2003.1228152.