ESCUELA NAVAL DE CADETES
"ALMIRANTE PADILLA"
Honor y Tradición

# REVISTA DERROTERO

## Seguridad y Defensa

# Modelo de evaluación y madurez de las capacidades de ciberdefensa para las fuerzas militares

Andrés Fernando Ortiz Alfonso [1]

[1]Suboficial del Ejército Nacional de Colombia, de grado Sargento Segundo, Ingeniero de Sistemas de la Universitaria de Colombia, Tecnólogo en Electrónica y Telecomunicaciones de la Escuela de Comunicaciones del Ejercito Nacional de Colombia. Contactos: (+57) 3008414833

**Recibido**: 20/08/2021
**Aprobado**: 04/10/2021

**Correspondencia:**
andres.ortizal
@buzonejercito.mil.co

**Citación**:
A. Ortiz-Alfonso. Modelo de evaluación y madurez de las capacidades de ciberdefensa para las fuerzas militares. Derrotero 15, número 1 (Ene-Dic) 2021.

**Resumen**

El presente documento tiene como propósito plantear una solución al problema de la evaluación de madurez de las capacidades esenciales en el ejercicio de la ciberdefensa, a través de un modelo que aborda un análisis comparativo de los diferentes manuales, guías y sistemas en el marco de la ciberdefensa, bajo una metodología y modelamiento que considera unas variables con niveles de medición; siendo adaptable a capacidades individuales y colectivas; contribuyendo a la toma de decisiones y proyección de esta disciplina, en búsqueda del fortalecimiento de las políticas, gobernanza, jurisprudencia, gestión e inversión a corto, mediano y largo plazo, para hacer frente a cualquier tipo de amenaza y ataque cibernético.

**Palabras clave:** ciberdefensa, ciberseguridad, modelo, madurez, capacidades.

ISSN: 2027-0658 | E-ISSN: 2590-4701

# Assessment and maturity model of cyber-defense capacities for the military forces[I]

**Abstract**
The purpose of this document is to propose a solution to the issue concerning the evaluation of the maturity of essential capabilities in the exercise of cyber defense. It is made through a model that addresses a comparative analysis of the different manuals, guides and systems in the framework of cyber defense, under a methodology and modeling that considers variables with measurement levels; therefore, it is adaptable to individual and collective capacities and it contributes to the decision-making and projection of this discipline, in search of the strengthening of policies, governance, jurisprudence, management and investment in the short, medium and long term, to face any type of threat and cyberattack.

**Keywords:** cyber defense, cybersecurity, model, maturity, mapabilities.

## Introducción

La ciberdefensa tiene una visión defensiva y ofensiva dentro del ciberespacio, para contrarrestar los diferentes ciberataques y ciberamenazas, siendo estos cambiantes en el tiempo, trayendo afectaciones críticas y dejando vulnerable al Estado; por ende, esta disciplina es liderada por las fuerzas militares y descrita en una normatividad (Departamento Nacional de Planeación, 2016); es importante tener un modelo de madurez dada por la necesidad de una métrica de Estado, con unas capacidades esenciales, con niveles de madurez que aporten a la proyección de las unidades cibernéticas militares; por tal motivo en el marco de la investigación se realiza la exploración y análisis dentro de la literatura existente que aporte los conocimientos necesarios para el desarrollo de los elementos que articulan el diseño del modelo de madurez.

Este artículo se divide en cuatro partes. La primera contiene el estado del arte de los modelos/guías y sistemas de capacidades de ciberdefensa, la segunda parte, muestra las capacidades de ciberdefensa esenciales definidas de la comparación y análisis anterior. La tercera parte identifica y caracteriza diferentes modelos de madurez cibernética, para proponer unos niveles de madurez que expliquen el estado actual de las capacidades cibernéticas; la cuarta, presenta el diseño articulado del conjunto de variables para realizar el modelo de evaluación, con su respectiva estructura de aplicación. Al final se plantean las conclusiones de la investigación.

[I] El presente artículo de investigación es presentado como opción de grado para optar al título de Magíster en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra, siendo producto del proyecto de investigación titulado *Modelo de evaluación de madurez de capacidades de ciberdefensa*.

# Metodología

Se realizó una investigación de los modelos y niveles de madurez de tipo cibernético, guías y sistemas de capacidades de ciberdefensa adaptables a las fuerzas militares, se realiza una comparación de los mismos y se definen las capacidades esenciales que debe contener el modelo planteado; donde se continua con la definición de las variables, con su respectivo nivel para la ejecución de la evaluación, dando como resultado un modelo esencial para el desarrollo de la ciberdefensa.

## 1. Capacidades en ciberdefensa

Se identificaron y contextualizaron las capacidades esenciales que surgen de la indagación y paridad de los documentos *National Cyber Security Framework Manual* (OTAN-CCDCOE, 2012), el Sistema Integral de Ciberdefensa-2020 (Comando Conjunto Cibernético, 2018) y la Guía de Ciberdefensa (Junta Interamericana de Defensa, 2020), un destacado referente en la materia que presenta las directrices y normas esenciales para el desarrollo de la ciberdefensa dentro de las unidades cibernéticas de las fuerzas militares de cualquier país.

La tabla **I** compila y describe las capacidades/subcapacidades de los documentos mencionados, donde se definen cinco categorías esenciales que debe tener una unidad de ciberdefensa para una buena ejecución y desarrollo de procesos de ciberdefensa, tabla primordial para el desarrollo del modelo de evaluación planteado.

## Modelos de evaluación de madurez

Se analizaron y compararon los modelos de madurez de tipo cibernético adaptables a la ciberdefensa, evaluar.

Se define como modelo de evaluación de madurez al conjunto de atributos e indicadores que representan la capacidad y el progreso de una disciplina específica, incluyendo normas y directrices en la práctica de la materia y cuyo objetivo principal es cuantificar las tareas desarrolladas, hacerlas medibles, logrando la madurez en el tiempo (Goksen, Cevik, & Avunduk, 2015), midiendo la progresión y alcanzando las diferentes cualidades propias de cada nivel (Rea-Guamma, Sanchez, Feliu, & Calvo, 2017); su aplicación permite planear lo que se debe lograr para llegar a donde se quiere ir, gestionar el crecimiento y la evolución organizacional, y corregir si se está desviando el rumbo; en últimas, saber qué se está haciendo, cómo se está haciendo, cómo se puede mejorar (Arbelaez, 2017). Los modelos de madurez se clasifican en tres tipos como se describe en la tabla **II**.

**Tabla I.** Capacidades/subcapacidades para el modelo de evaluación

| **Ofensiva cibernética** | | | |
|---|---|---|---|
| Grupo de capacidades militares esenciales realizadas en el ciberespacio para destruir/alterar/interrumpir los diferentes puntos/blancos determinados, objetivos de alto valor para el Estado, dentro del desarrollo de las operaciones militares, con la finalidad de defender la soberanía e integridad del territorio nacional. | | | |
| **Capacidades** | **Definición** | **Subcapacidades** | **Definición** |
| Ciberataque | Empleo deliberado de ciberarmas automáticamente o por personas, generando daños y efectos en redes/sistemas/físicos en objetivos y condiciones específicas. | | |
| Ciberarmas | Software diseñado a la medida y para objetivos estratégicos/operacionales (redes/sistemas del adversario), con munición (exploit/troyanos/etc.) efectuando daños/efectos proyectados e inesperados. | | |
| Ciberriesgo | Proceso dinámico continuo en la gestión de procesos donde hay probabilidad de impacto, ciberataque o explotación de una vulnerabilidad, en un sistema u objetivo de alta criticidad. | | |
| Ciberdisuación | Habilidad de pasar de víctima a ser potencial amenaza (capacidades de contraataque). Absteniendo al adversario de iniciar un ataque. | | |
| Cibertácticas | Empleo de ejercicios tácticos-operativos para obtener ventaja estratégica ante una ciberoperación ofensiva, defensiva o de apoyo. | Reconocimiento del ciberterreno | Identificación de la topología y vulnerabilidades del adversario. |
| | | Grupos especiales cibernéticos | Grupos pequeños de personas con capacidades y elementos necesarios en ejecución de ciberataques específicos. |
| | | Ciberinfiltración | Acceso clandestino a los sistemas/redes del adversario en cumplimiento de una ciberoperación específica. |
| | | Cibervigilancia | Actividades de monitoreo en las redes propias con la finalidad de evitar una ciberamenaza. |
| | | Ciberemboscada | Realizada mediante ciberseñuelos (redes-trampa/honey-pots.), buscando el efecto de una trampa para el adversario. |
| | | Ciberseñuelos/redes trampa | Uso de dispositivos de red aislados simulando la red real, con el objetivo captar la atención del adversario evitando un ciberataque. |
| | | Plataformas de ciberdecepción | Uso de plataformas automatizadas/dinámicas de redes-trampa con capacidades de detectar/analizar/bloquear ciberataques. |
| | | Fuego y movimiento cibernético | Desarrollo de elementos necesarios para ser empleados después de realizar un ciberataque sin dejar rastro ni de las tips usadas/ni del atacante. |
| Operaciones ofensivas | Operaciones desarrolladas en marco de un conflicto, en la topología del adversario generando daños físicos o ciberefectos. | De respuesta | Ejecutadas sobre el adversario, para prevenir/anticipar/reaccionar ante un ciberataque. |
| | | Preventivas de respuesta | Ejecutadas sobre el adversario que, por información de inteligencia, va realizar un ataque próximo o futuro. |
| | | Anticipadas de respuesta | Ejecutadas sobre el adversario que, por información de inteligencia, está por ejecutar un ataque inminente. |
| | | De falsa bandera | Ejecutadas de manera oculta, con el objetivo de culpabilizar a un tercero. |
| | | Reactivas de respuesta | Ejecutadas sobre el adversario que está ejecutando un ciberataque en curso. |

| **Defensa cibernética** | | | |
|---|---|---|---|
| Grupo de capacidades militares esenciales para contener/mitigar las posibles ciberamenazas, detectar ciberintrusiones y efectos de operaciones cibernéticas adversas, con la finalidad de proteger los activos cibernéticos y usuarios en la red propia. | | | |
| **Capacidades** | **Definición** | **Subcapacidades** | **Definición** |
| Ciberresiliencia | Adaptación/reacción de la unidad cibernética en continuar labores a pesar de ocurrir un ciberevento adverso. | | |
| Gestión de la ciberseguridad | Manejo y gestión de eventos de ciberseguridad en conjunto con las unidades de ciberseguridad (SOC-NOD-SCIRT). | | |
| Operaciones defensivas | Operaciones realizadas en redes propias en busca de vulnerabilidades y ciberriesgos. | Defensivas pasivas | Ejecutadas en la red propia, con el objetivo de prevenir/proteger y generar resiliencia. |
| | | Defensivas activas | Ejecutadas en redes propias, de tipo intrusivas (test de penetración, hacking ético) en busca de vulnerabilidades y ciberriesgos. |
| | | Defensa colectiva | Ejecutadas en redes aliadas y con consentimiento, con la intención de realizar ejercicios tácticos e identificar riesgos desde redes públicas. |
| Ciberdefensa avanzada | Habilidades para el monitoreo/análisis y evaluación Amenazas Persistentes Avanzadas - APT. | Defensa contra terceros | La gestión del riesgo de terceros dentro del suministro/distribución/operación/mantenimiento de las tecnologías propias de la unidad. |
| | | Caza de ciberamenzas | Habilidades en software para el manejo de ciberamenazas, orientado a la detección/bloqueo/análisis y aislamiento de amenazas avanzadas (APT). |

| **Inteligencia cibernética** | | | |
|---|---|---|---|
| Grupo de capacidades esenciales que despliegan todas las habilidades y recursos de inteligencia para la recopilación/difusión/explotación de diferentes fuentes de datos públicas, dando soporte a las actividades u operaciones militares en el ciberespacio. | | | |
| **Capacidades** | **Definición** | **Subcapacidades** | **Definición** |
| Inteligencia y contrainteligencia cibernética | La aplicación del ciclo de inteligencia militar a nivel operativo, táctico y estratégico a objetivos en busca de información de valor estratégico/operacional para la protección y defensa de la nación. | | |
| Inteligencia colectiva | Cooperación nacional/internacional en ciberinteligencia (plataformas compartidas o en cooperación para el manejo de la información) para la protección y casería de ciberamenazas. | | |
| Inteligencia de ciberamenzas | Manejo de amenazas complejas, destructivas y/o coercitivas internas y externas, en adaptación con el monitoreo, la investigación y el análisis en las ciberoperaciones. | Amenazas internas externas | Habilidades en la protección y conocimiento mediante software para la prevención de ciberataques por posibles ciberamenazas declaradas. |
| | | Amenaza persistente avanzada | Habilidades en software para el monitoreo, análisis e investigación del comportamiento de las amenazas de tipo avanzado en redes propias o externas. |

| **Excelencia cibernética** | | | |
|---|---|---|---|
| Grupo de capacidades esenciales para el desarrollo de la ciberdefensa en el tiempo con los recursos humanos, administrativos, logísticos, de doctrina y de jurisprudencia necesarios para el buen uso del ciberespacio y protección de la nación. | | | |
| **Capacidades** | **Definición** | **Subcapacidades** | **Definición** |
| Logística cibernética | Habilidades propias para los procesos y métodos en la ejecución de aspectos económicos, administrativos, presupuestales, técnicos y logísticos. | | |
| Doctrina cibernética | Habilidades en marco doctrinal militar, estableciendo principios, valores, directrices y normas de seguridad y confianza digital; fundamentales en el actuar cibernético dentro de los cuatro dominios de la guerra (tierra/mar/aire/espacio). | | |
| Marco legal cibernético | Habilidad en la generación de políticas, legislación, instrucciones y técnicas en ciberdefensa de tipo ofensivo/defensiva en el marco de los derechos humanos, la gobernanza y las actuaciones propias del ciberespacio. | | |
| Cooperación cibernética | Habilidades para una ciberdefensa sólida y a la vanguardia en cooperación en el ámbito nacional e internacional (aliados estratégicos, relaciones multilaterales con la Organización del Tratado del Atlántico Norte (OTAN) y la Junta Interamericana de Defensa (JID), el sector industrial-académico, buscando el buen uso del ciberespacio. | | |
| Educación cibernética | Formación del talento humano, otorgando capacidades para mantener el conocimiento y el desarrollo de la ciberdefensa a la vanguardia. | Adiestramiento cibernético | Habilidades en recursos tecnológicos y personal para realizar capacitaciones y ejercicios prácticos con el personal de toda la organización. Creando conciencia colectiva. |
| | | Educación cibernética individual | Habilidades en software y personal para capacitar y certificar las unidades cibernéticas, y ofrecer planes de educación al personal con el objetivo de mantener la ciberdefensa a la vanguardia. |
| | | Educación Cibernética Cooperativa | Habilidades en software y personal en ejercicios colectivos de adiestramiento cibernético, aumentando la capacidad de la unidad cibernética |
| Talento humano cibernético | Habilidades en la gestión y administración del talento humano (planes/procesos/procedimientos) con la finalidad de mantener las capacidades en un alto nivel. | Plan de carrera | Habilidades en la gestión, directrices para la realización de una especialidad cibernética que ayude a mantener el talento humano. |
| | | Gestión del talento humano | Habilidades en directrices, temas de bienestar, primas y manejo del personal. |
| | | Gestión del conocimiento | Habilidades propias de la unidad para el manejo del personal mediante normas y directrices por área funcional de la unidad. |
| | | Consagración del talento humano | Habilidades en directrices, normas y procedimientos para la fidelización y el bienestar del personal en educación. |

| **Soporte tecnológico cibernético** | | | |
|---|---|---|---|
| Grupo de capacidades que garantizan los recursos tecnológicos, de seguridad y protección digital necesarios para ejercer una correcta ciberdefensa y sostener un ciberespacio óptimo. | | | |
| **Capacidades** | **Definición** | **Subcapacidades** | **Definición** |
| Acondiciona-miento cibernético | Capacidades en ambientes físicos propios, áreas de tipo confidencial acondicionadas con las normas, tecnología y seguridad cibernética en desarrollo de operaciones y ejercicios cibernéticos. | | |
| Soporte TI | Habilidades en hardware-software que soportan y mantienen las plataformas de la unidad cibernética en desarrollo de las ciberoperaciones. | Conectividad | Capacidades de en topología herramientas de red, redes lan/wan, centros de cableado. |
| | | Almacenamiento/ sistemas de backup | Capacidades de la unidad cibernética en manejo y empleo de tecnologías para el manejo de información y software, en función de la unidad. |
| | | Aplicaciones servicios y sistemas | Capacidades propias de la unidad cibernética, la cual cuenta con su propio data center, máquinas de hiperconvergencia, sistemas de virtualización, y software que sostiene y mantiene la unidad cibernética funcionando. |
| Innovación cibernético | Habilidades en laboratorio / hardware/software para la innovación/desarrollo y ejecución, actualización de productos y tecnología existente, manejo de I+D+I. | Investigación y desarrollo cibernético | Capacidades en infraestructura, laboratorios o centros de investigación, para la innovación y desarrollo de software a la medida y necesidades propias de la unidad. |
| | | Observatorio tecnológico cibernético | Trabajo cooperativo (público-privado/nacional-internacional, fabricantes de software y unidades cibernéticas) para la investigación de tecnologías avanzadas y emergentes. |

**Fuente**: elaboración a partir de los modelos investigados (Junta Interamericana de Defensa, 2020, OTAN-CCDCOE, 2012, Comando Conjunto Cibernético, 2018)

**Tabla II.** Tipos de modelos de madurez

| | |
|---|---|
| **Progresión** | Describe los niveles como el estado de éxito más alto que puede alcanzar. |
| **Capacidad** | Muestra los niveles como la medida de un conjunto particular de prácticas a seguir. |
| **Híbrido** | Unión de los dos anteriores. Integrando el logro y capacidad en una sola particularidad. |

**Fuente**: (Le y Hoang, 2016).

Los modelos que se adaptan a la investigación son de tipo híbrido, ya que para la ciberdefensa se puede decir que no hay modelos definidos; por ende, se listaron los modelos más utilizados a nivel cibernético, así:

- **CMM (Capability-Maturity-Model).** Evalúa la calidad del software en desarrollo, mantenimiento y operación de la madurez en función de los procesos, el cual contie-

ne cinco niveles de evaluación: (1) inicial, (2) repetible, (3) definido, (4) gestionado, (5) optimizado. Cada nivel contiene los requisitos de madurez específicos para su desarrollo (Le y Hoang, 2016), teniendo en cuenta la implementación de los procesos y requisitos de calidad necesarios para alcanzar la madurez del nivel y sucesivamente todos los niveles, siendo un modelo base usado para muchos proyectos y desarrollo de software.

- **CCSMM (Community-Cyber-Security-Maturity-Model).** El modelo de madurez comunitario de la seguridad cibernética, creado por Dr. Gregory B. White, desarrollado en Texas, (White, 2007), está enfocado bajo un modelo holístico, determinando la postura de la ciberseguridad en las organizaciones, y las diferentes naciones o comunidades, trabajando a nivel de esfuerzo comunitario (Rea-Guamma, Sanchez, Feliu, & Calvo, 2017), el cual contiene la geografía con tres escalas que incluyen organización, comunidad y Estado, compuesto por cinco niveles: (1) inicial, (2) avanzado, (3) autoevaluado, (4) integrado, (5) vanguardia (Le y Hoang, 2016).

- **CSF-NIST (Cyber-Security-Framework).** Definido como un marco de referencia de ciberseguridad, desarrollado por la NIST-2014, donde se contempla un conjunto de tareas para perfiles individuales en la operación (Le y Hoang, 2016), centrado en el seguimiento de progresos de la organización en su ejecución, pasando del estado actual al objetivo definido. Este modelo establece cinco niveles: (1) identificar, (2) proteger, (3) detectar, (4) responder, (5) recuperar (Almuhammadi y Alsaleh, 2017).

- **C2M2 (Cybersecurity-Capability-Maturity-Model).** Modelo enfocado al sector energético, orientado a la administración e implementación de prácticas de ciberseguridad, entrelazando las tecnologías de la información (TI), tecnologías de operaciones (OT) y entornos en que operan (DOE & Energy, 2014). Incorporando una escala de tres niveles: (0) no realizado, (1) iniciado, (2) realizado, (3) gestionado.

- **SSE-CMM (Systems-Security-Engineering-Capability-Maturity-Model).** Se definen los componentes necesarios para los procesos de ingeniería de sistemas que deben existir dentro de una organización, creado por la agencia de seguridad nacional de EEUU-2001, definiendo cinco niveles de madurez: (1) realizado informalmente, (2) planificar rastrear, (3) bien definido, (4) control, (5) mejoras continuas (Goksen, Cevik, & Avunduk, 2015).

- **CMMI (Capability-Maturity-Model-Integration).** Este modelo es una integración del modelo CMM y SE-SMM para la mejora de los procesos en todos los ámbitos y niveles de las organizaciones, que facilita y adopta varios procesos en uno solo, e integra su contenido y evolución en los procesos, dando guía para la estrategia en

la mejora continua; se define en seis niveles: (0) incompleto, (1) ejecutado, (2) gestionado, (3) definido, (4) cuantitativamente gestionado, (5) optimizado (Villa, Ruiz, & Ramos, 2004). También incorpora dos tipos: el modelo continuo, enfocado a cada área de proceso, medido de forma individual; y el modelo por etapas, buscando el nivel de madurez organizacional dividido en un mapa predefinido, basado en procesos justificados y organizados relacionalmente (Villa, Ruiz, & Ramos, 2006).

A continuación, se confrontan los modelos investigados en la tabla **III**, los cuales están adaptados con apartes basados en temáticas cibernéticas.

**Tabla III.** Comparación de los modelos de madurez

| Modelo de madurez | | Aspectos importantes | Niveles de madurez | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | CMM | Adaptable/integrable con múltiples disciplinas y buenas prácticas. | | Inicial | Repetible | Definido | Administrado | Optimizado |
| 2 | CCSMM | Tipo comunitario, enfocado a la ciberseguridad de apoyo. | | Inicial | Avanzado | Autoevaluado | Integrado | Vanguardia |
| 3 | CSF-NIST | Enfocado a la infraestructura federal. | | Identificar | Proteger | Detectar | Responder | Recuperar |
| 4 | C2M2 | Enfocado al sector energético con gestión de infraestructura crítica. | No realizado | Iniciado | Realizado | Gestionado | | |
| 5 | SSE-CMM | Aplicado a la seguridad de la información, usado en trabajos de investigación. | | Realizado informalmente | Planificar y rastrear | Bien definido | Control | Mejoras continuas |
| 6 | CMMI | Modelo integrado a la mejora con estrategia de mejora continua. | Incompleto | Ejecutado | Gestionado | Definido | Cuantitativa mente gestionado | Optimizado |

**Nota:** desarrollado a partir de los modelos investigados.

En conclusión, se aprecia que estos modelos comparten elementos comunes del modelo CMM y CMMI, por su factibilidad y adaptabilidad; por ende, se realizó una adaptación de los niveles de madurez para la investigación, descritos en la tabla **IV**.

**Tabla IV**

| Nivel de madurez | Denominación del nivel | Definición |
|---|---|---|
| 0 | No comprobado/aplicado | No es observado o no aplica |
| 1 | Preliminar | informal/reactivo |
| 2 | Gestionado | Controlado a nivel planificación y evaluación |
| 3 | Definido | Dinámico/Proactivo |
| 4 | Controlado y gestionado | Medido controlado |
| 5 | Optimizado | Estable-Flexible |

**Nota:** adaptado de los modelos CMM/CMMI.

**Tabla V.** Caracterización de cada nivel de madurez

| |
|---|
| (0) No comprobado/ No aplicado |
| • Cuando la capacidad no es tenida en cuenta o cumplida dentro de las capacidades de la unidad. |
| (1) Preliminar |
| • Contemplada como necesidad, pero no se tiene algo concreto.<br>• No existe algo planeado, manejada en ambiente impredecible y reactivo por la necesidad.<br>• Solución específicamente para el problema o fin (Tipo ad-hoc).<br>• Se encuentra en un estado sin presupuesto (no es contemplado como una necesidad).<br>• Carece de un ambiente estable que de soporte.<br>• Alcanza éxito por esfuerzos heroicos/individual, sin apoyo.<br>• Alcanzan el propósito de manera inconsistente (no es planeada-sin seguimiento/medición).<br>• El éxito en su empleo no es seguro. |
| (2) Gestionado |
| • Planeada y ejecutada teniendo en cuenta políticas/procedimientos/normatividad.<br>• Satisface descripciones/procesos/estándares/procedimientos definidos.<br>• Se tiene una base gestionada, pero no suficiente.<br>• Presenta algunos problemas en su implementación/aplicación.<br>• Para su gestión, el tiempo/costos/recursos son factibles, pero limitados.<br>• Tiene salidas controladas y estables.<br>• Tiene documentación básica.<br>• Susceptible de mejora en sus procesos<br>• Gestionado a nivel proyecto.<br>• Es planeada con seguimiento.<br>• Se miden productos, pero no servicios.<br>• Se proyecta el presupuesto. |
| (3) Definido |
| • Bien caracterizado por estándares/procedimientos/herramientas/métodos rigurosos, pero sin seguimiento.<br>• Se tiene algo establecido (satisfaciendo la necesidad), se espera mejorar con el tiempo.<br>• Aplican la mejora de procesos en nivel definido.<br>• Es estable y consistente. |
| • Estandarizado/basado en buenas prácticas.<br>• Cuenta con planes de capacitación (habilidades y conocimiento de acuerdo con roles).<br>• Facilitan la reducción de costos/tiempo/recursos.<br>• Medición en categoría productos y servicios.<br>• Cuenta con modelos de estimación.<br>• Tiene presupuesto limitado. |
| (4) Administrado y gestionado |
| • Necesidad cubierta, con mejora constante/seguimiento/análisis/control cualitativo y cuantitativo.<br>• Capacidad cubierta para la necesidad.<br>• Contempla mejoras en la administración y gestión.<br>• Contempla presupuesto en sostenimiento en el tiempo.<br>• Plantea objetivos basados en mediciones.<br>• Es medible y controlado (Data-driven).<br>• Adaptado a la necesidad del usuario y organización.<br>• Capacidad y riesgo medible.<br>• Definición de metas de calidad del proceso y del producto.<br>• Cuantificable y predecible.<br>• Cumple con planes/programas de mejora.<br>• Obtiene productos de alta calidad.<br>• Uso de modelos predictivos.<br>• Identificación de brechas. |

| (5) Optimizado |
|---|
| • Estable y flexible.<br>• Aplicación en mejora continua/adaptación al cambio.<br>• Capacidad cubierta/desarrollada completamente a la necesidad, previendo sostenibilidad y mejora en el tiempo.<br>• Continuamente mejoran sus procesos/basados en entendimiento cuantitativo/cualitativo de los objetivos de la organización y necesidades |
| • Está en el nivel más alto en gestión y desarrollo.<br>• Implementa mejoras por medio de análisis y estrategias DOFA (debilidades, oportunidades, fortalezas y amenazas).<br>• Directivos con capacidad de estimar, hacer seguimiento cuantitativo al impacto/efectividad de los cambios.<br>• Mejora continua de proceso a la par de la madurez.<br>• Implementación en tecnologías y métodos nuevos.<br>• Cumplimiento de objetivos de calidad.<br>• Aplicación de métodos/procedimientos para cerrar brechas.<br>• El presupuesto es suficiente y sostenido en el tiempo. |

Se toma como referencia algunos apartes descritos en la evaluación del modelo SICID (Cabuya Padilla y Sierra Abril, 2019), donde para cada uno de los niveles de madurez ( de 0 a 5) se realiza una caracterización que ayudan a definir y dar claridad en el momento de realizar la evaluación de las variables como se muestra a continuación en la tabla **V**.

## Diseño articulado del conjunto de variables para realizar el modelo de evaluación planteado

Ya definidos los componentes capacidades/subcapacidades, escala de medición y caracterización de los niveles, se pasa a determinar las variables que evalúan cada capacidad/subcapacidad, finalizando con los factores que ayudan a determinar la aplicación de la evaluación.

Como elemento de juicio referente al nivel de madurez de una variable, se adopta la doctrina aplicada en la obtención de capacidades de las Fuerzas Militares basadas en los componentes de doctrina, organización, material, personal e infraestructura (DOMPI), (Capacitas-MDN, 2018), que ayudan a la toma de decisión en el nivel de madurez (0-5) de la variable a evaluar, como se describen en la tabla **VII**.

### *A. Estructura de aplicación*

Considerando todos los elementos aportados anteriormente, resulta el modelo de evaluación deseado; en su aplicación se estructura y organiza contestando la totalidad de las variables, considerando los siguientes aspectos:

- Área funcional: área definida para la evaluación de la capacidad/subcapacidad.
- Capacidad/Subcapacidad: habilidades del área-funcional a evaluar (tabla **VI**).

**Tabla VI.** Definición de variables por capacidad/subcapacidades

| **Ofensiva cibernética** | | |
|---|---|---|
| **Capacidad** | **Subcapacidades** | **Variables** |
| Ciberarmas | | Posee software o plataformas para desarrollar ciberarmas, diseñadas para la ejecución de un ataque dirigido a un blanco u objetivo de alto valor (puede ser estratégico, operacional o táctico) para la misión militar asignada, que puede ser una organización/persona/redes/sistema informático/base de datos/programa del adversario; por ende, unas condiciones específicas son tiempo/modo/lugar/tipo de ciberseguridad. |
| | | Cuenta con sistemas de ciberarmas (siendo un sistema que integra diferentes ciberarmas, algunas funciones en mando y control (apoyos técnicos necesarios para el desarrollo de una ciberoperación). |
| Ciberataque | | Cuenta con herramientas de tipo software (ejemplo un ataque de DDOS (Ataque de denegación de Servicios Distribuido) en servidor o correo del adversario) que ayudan al desarrollo de las fases de la cadena de la muerte (kill chain), para ejecutar ataques a objetivos estratégicos de manera ofensiva/defensiva, de ser necesario. |
| Ciberriesgo | | Cuenta con un sistema/modelo/proceso sistemático para investigar/identificar amenazas/vulnerabilidades en la red propia, identificando probabilidad/impacto que ayudan a la toma de decisiones previniendo posibles ciberataques. |
| | | Trabaja en cooperación con las unidades cibernéticas, investigando actividades cibermaliciosas, dando el entendimiento de los daños físicos y cibernéticos causados por organizaciones maliciosas; siendo documentadas y tenidas en cuenta para la toma de decisiones y mejora de procesos. |
| | | Se desarrolla y genera un plan de gestión del ciberriesgo. |
| Ciberdisuación | | Cuenta con una ciberdefensa robusta (elementos en software/hardware/personal de tipo ofensivo) para hacer frente a un ciberataque o una ciberguerra. |
| Cibertácticas | Reconocimiento del ciberterreno | Realiza ejercicios/operaciones de tipo inteligencia y herramientas de análisis de topología y vulnerabilidades de las redes del adversario en todas sus capas (modelo-OSI). |
| | Grupos especiales cibernéticos | Cuentan con la cooperación de grupos expertos de universidades/oficinas cibernéticas privadas, para ser reclutados en caso un ciberataque al Estado o una ciberguerra. |
| | | Cuentan con los recursos tecnológicos/económicos/personal idóneo (fuerza ciberespacial de ciberdefensa móvil). |
| | Ciberinfiltración | Cuenta con software/personal para generar acceso clandestino en redes internas y del perímetro del adversario para la identificación y neutralización de objetivos específicos. |
| | Cibervigilancia | Cuenta con hardware/software/personal para el monitoreo de las redes propias, en busca de comportamientos sospechosos y maliciosos. |
| | Ciberemboscada | Cuenta con software tipo señuelos (redes trampa/honeypots) plataformas de ciberdecepción, para la captura de ciberataques y ciberamenzas. |
| | Ciberseñuelos | Cuenta con software para sistemas de red virtuales aisladas (simulan entornos reales aislados) para contener posibles ataques adversarios para su análisis. |
| | | Cuenta con señuelos armados (códigos de software simulando información de interés), diseñados para capturar el interés del adversario, siendo activados en una exfiltración en ejecución de una ciberoperación. |
| | Plataformas de ciberdecepción | Cuenta con herramientas/software basadas en redes trampa/avanzadas/automatizadas para detectar y analizar en tiempo real ciberataques avanzados/día cero. |
| | Fuego y movimiento cibernético | Cuenta con software y hardware para el diseño y ejercicios de ciberataques (plataformas de simulación) con efecto de no ser detectados ni dejar rastro de las TIC (tecnologías de la información y las comunicaciones) usadas y el atacante. |

| | | |
|---|---|---|
| Operaciones ofensivas | Operaciones ofensivas de respuesta | Cuenta con software y personal para ejecutar operaciones ofensivas en redes adversarias para anticipar/prevenir ataques en redes propias. |
| | Operaciones ofensivas preventivas de respuesta | Cuenta con software/personal/inteligencia propia y aliada para evitar un ataque planeando o futuro. |
| | Operaciones ofensivas anticipadas de respuesta | Cuenta con software/personal para realizar acciones ofensivas contra el adversario que se considera un ciberataque inminente. |
| | Operaciones ofensivas de falsa bandera | Realiza operaciones encubiertas (redes aisladas) con alto valor de inteligencia, con intención de culpabilizar a un tercero. |
| | Operaciones ofensivas reactivas de respuesta | Cuenta con software/hardware/personal para ejecutar acciones de repeler ataques en curso. |
| **Defensa cibernética** | | |
| **Capacidad** | **Subcapacidades** | **Variables** |
| Ciberresiliencia | | Cuenta con métodos/procedimientos/software para mantener (anticipación de un ataque, manteniendo las actividades sin inconveniente operativo) la funcionalidad de la redes y actividades. |
| Coopera con las unidades de ciberseguridad nacionales/internacionales en ciberejercicios y actividades para mantener la mentalidad reactiva, aumentando las capacidades de reacción-anticipación de ciberataques. | | |
| Cuenta con la colaboración de un Centro de Operaciones cibernéticas -SOC /Centro de operaciones de Red - NOC / Equipo de Respuesta a Incidentes de Seguridad Informática - CSIRT / Equipo de Respuesta (o preparación) para Emergencias Informáticas. - CERT frente a las ciberamenazas y actividades que afecten la ciberseguridad de las redes propias con acciones de proteger/detectar/responder/recuperar. | | |
| Operaciones defensivas | Operaciones defensivas pasivas | Cuenta con software/hardware para realizar acciones de prevención/protección/resiliencia en las redes propias (mínimo una o dos veces al año). |
| | Operaciones defensivas activas | Tiene software (herramientas de threat hunting)/hardware para realizar acciones intrusivas (ingresos no autorizados)/ofensivas en las redes propias para prevenir posibles vulnerabilidades/riesgos. |
| | Operaciones defensa colectivas | Cuenta con defensa/colectiva (cooperación de países aliados y unidades cibernéticas) en acciones de defensa contra ciberamenazas avanzadas descritas en procesos y métodos. |
| Ciberdefensa avanzada | Defensa contra terceros | Cuenta con métodos y software para el control del personal externo que debe manipular las plataformas en beneficio de la infraestructura propia de la unidad cibernética. |
| | Caza de ciberamenazas | Cuenta con metodologías en ciberamenazas basadas en datos como Mitre-att&ck (información/técnicas/procedimientos). |
| **Inteligencia cibernética** | | |
| **Capacidad** | **Subcapacidades** | **Variables** |
| Inteligencia de ciberamenazas | Realizados en ejercicios colaborativos (público-privado), con métodos/procedimientos de información en ciberataques/sufridos/cercanos/cadena de ciberexterminio (kill-chain), siendo lecciones aprendidas. | |
| | Cuenta con métodos/procedimientos definidos en manejo de la desinformación/noticias falsas/manejo de la verdad frente a la ciberinteligencia. | |
| | Realiza acciones procedimientos en el aseguramiento y protección de la propiedad intelectual, evitando el ciberespionaje. | |
| | Amenazas internas externas | Cuenta con métodos/modelos y software para el monitoreo/análisis/detección de amenazas-conocidas e inesperadas en la red propia. |
| | Amenaza persistente avanzada | Cuenta con software para cacería de huella cibernética (siendo el rastro de algún acceso malintencionado a la red o equipos) realizando análisis forenses en el monitoreo, investigación, manejo de las posibles Amenazas Persistentes Avanzadas - APT, sea interno/externo de las redes propias y del adversario. |

| | | |
|---|---|---|
| Inteligencia y contrainteligencia cibernética | | Maneja el ciclo de inteligencia de amenazas para su uso interno/externo en la red propia y objetivos definidos en una ciberoperación. |
| | | Se aplican directivas o normas (en ejercicios y actividades de inteligencia y en ciberoperaciones) para el manejo de los métodos de inteligencia. |
| | | Cuenta con fuentes externas para el conocimiento de amenazas/presentes/nuevas/en desarrollo de una defensa activa y protección de redes propias. |
| Inteligencia colectiva | | Cuenta con la cooperación/corresponsabilidad nacional-internacional (OTAN/JID/INTERPOL/OEA/UNDOC/FID) mediante acuerdos/métodos/aplicaciones compartiendo información/inteligencia que ayuda a la planificación de ciberoperaciones conjuntas. |
| **Excelencia cibernética** | | |
| **Capacidad** | **Subcapacidades** | **Variables** |
| Logística cibernética | | Maneja recursos propios asignados a la unidad cibernética mediante recurso definido y exclusivo para la unidad cibernética, para la compra de herramientas cibernéticas, su funcionamiento y compra emergente en caso de un ciberataque, y otro recurso para la innovación tecnológica/educación. |
| Doctrina cibernética | | Cuenta con procesos y procedimientos en asesoramiento, cooperación, jurídica, financiera, gestión del conocimiento, lecciones aprendidas, para la toma de decisiones ante las autoridades competentes, y toma de decisiones a nivel de superior jerárquico. |
| | | Cuenta con los procesos y estrategia definida para la aprobación jerárquica que ayuden a la destinación de recursos, dejando claro la relación costo-beneficio. |
| | | Realiza creación de documentos, directrices en políticas, criterios, referencias, principios relativos y transversales para la ejecución de la ciberdefensa local, conjunta nacional e internacionalmente. |
| Marco legal cibernético | | Realiza la creación de políticas, DDHH cibernéticos en actividades de ciberdefensa de tipo nacional e internacional por medio de mesas de trabajo y plataformas comunitarias. |
| | | Cuenta con el personal jurídico en conocimientos cibernéticos, para la toma de decisiones y ejecución de la ciberdefensa operativa y administrativa de la unidad. |
| | | Ejecuta instrumentos legales, normas y guías relacionadas con la aplicación de los DIH en el ciberespacio. |
| | | Cuenta con métodos de control (compartir información del NIST cybersecurity framework) compartiendo información de ciberamenazas, realizando métodos, planes defensivos y ofensivos dentro y en relación con las unidades cibernéticas. |
| | | Cuenta con procesos y procedimientos para el manejo y asignación de recursos financieros, ordinarios, atípicos, en desarrollo de las operaciones cibernéticas. |
| Cooperación cibernética | | Cuenta con plataformas/software compartido con unidades militares cibernéticas, aplicando los principios y metodología de NIST cybersecurity framework para el manejo de información de inteligencia de amenazas/ciberataques. |
| | | Cuenta con plataformas, foros, conferencias con grupos de ciberdefensa (JID/OTAN/OEA/INTERPOL/UNDOC/FID) en la generación y creación de políticas, directrices, lineamientos multilaterales en caso de una ciberguerra. |
| | | Realiza procesos, métodos como NIST cybersecurity framework en protección de las infraestructuras críticas y actividades de innovación cibernética, en cooperación público-privada mediante plataformas, software o foros. |

| | | |
|---|---|---|
| Educación cibernética | Adiestramiento cibernética | Crean o manejan planes para el desarrollo, la concienciación en ciberamenazas/ciberdefensa en audiencias directas, generales y específicas de las unidades cibernéticas y fuerza militares. |
| | Educación cibernética individual | La unidad cibernética tiene planes y procesos definidos para la educación basados en los cargos, en formación especial permanente en niveles (operativos/técnicos/administrativos/tácticos/operacional/estratégicos/ políticos). |
| | | La unidad cibernética cuenta con planes, procedimientos y plataformas para la ejecución de ciberejercicios, de carácter técnico-procedimental, a niveles del mando en facetas (defensa/explotación/ofensiva), definiendo criterios y certificando las unidades cibernéticas. |
| | | La unidad cibernética tiene una hoja de ruta/planes/directrices recursos aplicados en la formación académica al personal dependiendo el cargo, aportando conocimientos/certificaciones a nivel táctico/operacional/estratégico. |
| | Educación cibernética cooperativa | La unidad cibernética tiene plataformas o software, planes y procedimientos para la realización de ejercicios colectivos nacionales en facetas de adiestramiento en tareas, ejercicios, evolución y certificación del grado de preparación de las unidades cibernéticas. |
| Talento humano cibernético | Plan de carrera | Tiene un plan de carrera de acuerdo con la especialidad, en progresión de carrera dentro de las fuerzas militares ayudando a reclutar, formar, capacitar y retener al personal. |
| | Gestión del talento humano | Consideran la administración de los recursos, pagos de primas y la logística necesaria al personal uniformado como de orden público, por el manejo de operaciones cibernéticas, bajo una directiva, plan o método. |
| | Gestión del conocimiento | Manejan procesos y procedimientos para la gestión del conocimiento del personal, en área funcional y técnica en operaciones desarrolladas por la unidad. |
| | Consagración del talento humano | Manejan planes de bienestar, formación, retención (en cada nivel de educación y rango) con traslados dentro de las unidades cibernéticas, garantizando el nivel de capacidades e inversión. |
| **Soporte tecnológico cibernético** | | |
| **Capacidad** | **Subcapacidades** | **Variables** |
| Soporte-TI | Conectividad | Cuenta con centros de redes propios, con componentes de red (switch/módems/canales de internet/routers) administrados para el desarrollo de las funciones propias de la unidad. |
| | Almacenamiento y backup | Cuenta con sistemas de almacenamiento (SAN/NAS/hiperconvergencia/nube) para el manejo de información/herramientas/servicios para el desarrollo de las actividades y ciberoperaciones. |
| | Aplicaciones servicios y sistemas | Cuenta con los elementos de software y hardware necesarios para facilitar, mantener y sostener las plataformas o software de ciberdefensa, en cumplimiento de labores propias de la unidad cibernética. |
| | Protección y seguridad cibernética | Cuenta con aplicaciones y software en las diferentes capas (modelo OSI, anillos de seguridad perimetral) para la protección de la red propia y acciones hostiles. |
| | Auditorias de seguridad TIC | Realiza auditorías de tipo operativo/técnico/seguridad en los sistemas de TI propios en busca de vulnerabilidades y posibles ciberamenazas. |

| | | |
|---|---|---|
| Innovación y análisis cibernético | Investigación y desarrollo cibernético | Coopera con las unidades de desarrollo tecnológico en la aplicación de I+D+I a nivel de ciberdelito y ciberdefensa mediante planes, foros y plataformas. |
| | | Realiza investigación y análisis en materia de industria cibernética, en función de los objetivos y lineamientos de la unidad, en la dominación del código y las herramientas, garantizando el uso adecuado, personalizado y continuo frente a las ciberarmas. |
| | | Manejan procesos y métodos para las tendencias, ayudando a tener anillos de seguridad avanzados basados en aspectos de seguridad de origen, confianza cero y seguridad de externos. |
| | | Desarrollan investigación propia (desarrollos sensibles/urgentes), ajena (desarrollos a largo plazo) y mixta (desarrollos complejos), dentro de un laboratorio tecnológico, dando nuevos o mejoras de software en los anillos de seguridad y defensa cibernética de la unidad. |
| | | Cuenta con plataforma, sistemas y personal en desarrollo de investigación en la gestión, control y evaluación de la eficacia de resultados a mediano y largo plazo, mejorando programas, productos nuevos y tecnología existente. |
| | Observatorio tecnológico cibernético | Cuenta con software, hardware, laboratorios, sistemas y /o modelos para probar, valorar y analizar productos y nuevas tecnologías en ciberdefensa. |
| | | Trabajan en cooperación nacional, internacional, industria y unidades cibernéticas para el avance tecnológico, empleando y buscando la mejora en la ciberdefensa avanzada y proactiva de tecnologías emergentes basadas en los temas principales: seguridad de origen, confianza cero y seguridad de externos. |
| Adecuación cibernética | | Cuenta con instalaciones propias, acondicionadas con material y equipos (laboratorios forenses, de investigación, de monitoreo y áreas administrativas). |
| | | Cuenta con ambientes confidenciales, acondicionados para operaciones cibernéticas y de alto grado (ultrasecreto), protegiendo la confidencialidad de la información. |
| | | Cuenta con ambientes encubiertos para la protección del anonimato en ciberoperaciones de tipo sensible, desvinculadas de las instalaciones u organismos públicos. |

**Tabla VII.** Componentes DOMPI adaptado a la ciberdefensa

| Niveles | Componentes de evaluación |
|---|---|
| Doctrina | Conjunto de instrucciones y normas que guían los métodos y/o procesos en desarrollo de la doctrina cibernética, en aspectos operativos, administrativos y organizacionales, en cumplimiento de la misión constitucional de las fuerzas militares. |
| Organización | Estructura funcional/espacial de las unidades cibernéticas, incluyendo funciones, estructura, protocolo organizacional, mando, coordinación y comunicación en la que los componentes posteriores interactúan coordinadamente para lograr su misión. |
| Material y equipo | Elementos necesarios para desarrollar, mantener y sostener actividades que contemplan el ciclo de vida del material y equipo (hardware/software de las plataformas tecnológicas, laboratorios y plataformas cibernéticos). |
| Personal | Grupo de uniformados/civiles requeridos para el cumplimiento de las tareas asignadas, contemplando el plan de carrera cibernética y el liderazgo individual. |
| Infraestructura | Conjunto de bienes inmuebles, instalaciones, redes de servicios, incluyendo la infraestructura en propiedad o tenencia para el desarrollo de la ciberdefensa. |

**Fuente:** Capacitas-MDN, 2018.

**Tabla VIII.** Ejemplo de aplicación de la estructura del modelo

| Área funcional | Capacidad | Subcapacidades | Variables | Estado actual | Estado ideal | Nivel de madurez |
|---|---|---|---|---|---|---|
| Ofensiva cibernética | Ciberarmas | | Posee software o plataformas para desarrollar ciberarmas diseñadas para la ejecución de un ataque dirigido a un blanco u objetivo de alto valor (puede ser estratégico, operacional o táctico), para la misión militar asignada que puede ser una organización, persona, redes, sistema informático, base de datos, programa del adversario, por ende, unas condiciones específicas que son tiempo/modo/lugar/tipo de ciberseguridad que posea. | Se tiene documentada preliminarmente, no se cuenta con el recurso humano, económico o jurídico para la adquisición o manipulación de la capacidad. | Se cuenta con el software, hardware, personal y doctrina en el empleo y manejo de esta capacidad. | Se encuentra en un Nivel 1. Preliminar. |
| | Cibertácticas | Ciberemboscada | Cuenta con software tipo señuelos (redes trampa/honey-pots.), plataformas de ciberdecepción para la captura de ciberataques y ciberamenazas. | Se cuenta con el software, documentación básica, recursos limitados, poco personal idóneo y la infraestructura adecuada, siendo casi reactivos en el uso de esta capacidad. | Se tiene el software (Honey-Pots), infraestructura y procedimientos claros, personal experto para el manejo de esta herramienta. | Se encuentra en un Nivel 2. Gestionado. |

- Variables: descripción a evaluar por cada capacidad/subcapacidad (tabla **VI**).
- Estado actual: expresa sintetizadamente el estado actual de la variable a describir, indicando y considerando los componentes DOMPI en los aspectos de recursos y tecnologías actuales con las que cuentan para desarrollar la capacidad. De no contar con la capacidad evaluada se escribe "no se cuenta con la capacidad".
- Estado ideal: expresa sintetizadamente el estado deseado de la variable a describir, indicando y considerando los componentes DOMPI en los aspectos de recursos y tecnologías ideales que requiere tener en esta capacidad.
- Nivel de madurez: teniendo en cuenta los componentes DOMPI y la caracterización (tabla **VII**), se evalúa la madurez (0-5) dentro del nivel seleccionado (tablas **IV** y **V**), en la tabla **VIII** a continuación se realiza un ejemplo asociado al área funcional de ofensiva cibernética:

En este mismo ejemplo, la evaluación de la capacidad se realiza tomando todos los valores de resultado individualmente, posteriormente se promedian teniendo en cuenta la cantidad de variables que tiene la capacidad; para el ejemplo son 6, dando el promedio total así, (1+2+3+3+1,8+1,2) /6= 2, si pasa de 2.5 se aumenta al siguiente nivel, por ende, queda en 2 la capacidad como se muestra en la tabla **IX** y la figura **1**.

**Tabla IX.** Calificación de la capacidad total

| área funcional | capacidad | Sub-capacidades | Sub-Prom | Prom-total |
|---|---|---|---|---|
| **Ofensiva Cibernética** | Ciberarmas | | | 1 |
| | Ciberataque | | | 2 |
| | Ciberriesgo | | | 3 |
| | Ciberdisuacion | | | 3 |
| | **Cibertacticas** | Reconocimiento del ciberterreno | 1 | |
| | | Grupos especiales cibernéticos | 3 | |
| | | Ciberinfiltración | 2 | |
| | | Cibervigilancia | 1 | 1,8 |
| | | Ciberemboscada | 3 | |
| | | Ciberseñuelos | 2 | |
| | | plataformas de ciberdecepción | 1 | |
| | | Fuego y movimiento Cibernético | 2 | |
| | **Operaciones Ofensivas** | Operaciones ofensivas de respuesta | 1 | |
| | | Operaciones ofensivas preventivas de respuesta | 2 | 1,2 |
| | | Operaciones ofensivas anticipadas de respuesta | 1 | |
| | | Operaciones ofensivas de falsa bandera | 1 | |
| | | Operaciones ofensivas reactivas de respuesta | 2 | |
| | **Total, Promedio** | | | 2 |

**Fuente:** elaborado a partir del modelo investigado (Cabuya Padilla y Sierra Abril, 2019).

## *B. Estrategia de medición de la madurez*

A continuación, se presenta las pautas principales a considerar en el desarrollo de la estrategia de medición de madurez:

- Sobre el "Estado actual" para la respuesta se debe considerar los componentes DOMPI ya que con ellos se da claridad y comprensión de los cinco elementos necesarios para una madurez, que para este caso serían:
    - ¿Qué se tiene de ciberarmas a nivel-doctrina? (procedimientos/manuales/ métodos de aplicación y adquisición).

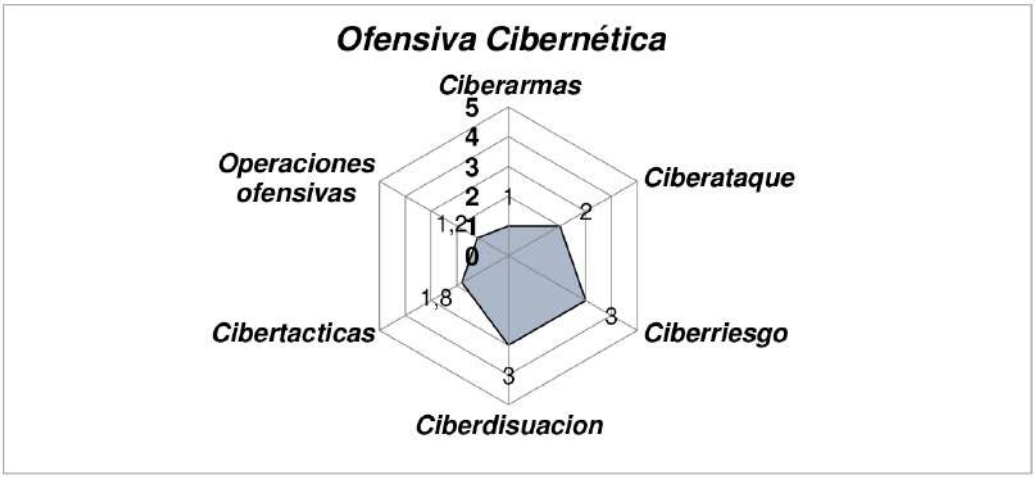


**Figura 1.** Gráfica del promedio de la capacidad

**Fuente**: elaborada a partir del modelo investigado (Cabuya Padilla y Sierra Abril, 2019).

- ¿Qué se tiene de ciberarmas en temas de organización? (¿Se cuenta con la logística, comunicación, niveles de mando, protocolos para el empleo y manejo de estas?).
- ¿Qué se tiene de ciberarmas en la dimensión de materiales/equipos? (¿Se cuenta con equipos, PC, servidor y/o software necesario para la obtención y funcionamiento de ciberarmas?).
- ¿Qué se tiene de ciberarmas en el aspecto de personal? (¿Se cuenta con el personal experto e idóneo para el empleo y ejecución de la capacidad?).
- ¿Qué se tiene de ciberarmas en el aspecto de infraestructura? (¿Se cuenta con un espacio físico secreto para el empleo de ciberarmas?).

- En el "Estado-Ideal" para la respuesta se consideran nuevamente los componentes DOMPI que describen la forma óptima de solventar la necesidad de la unidad cibernética referente a la capacidad evaluada.
- Para definir el nivel de madurez se consideran las tablas 3 y 4, que define cuáles son los niveles del modelo, y la tabla 5, que da una caracterización más clara de cada nivel de madurez. La tabla 10 toma la información del "Estado-Actual" y presenta las definiciones de los valores que toma la variable, con el fin de determinar un estado claro del nivel de madurez.

**Tabla X.** Extracto de la tabla del nivel de madurez y tabla de caracterización

| Nivel de madurez | Denominación del nivel |
|---|---|
| 0 | No comprobado/aplicado |
| 1 | Preliminar |
| 2 | Gestionado |
| **0 – No comprobado/No aplicado** | |
| Cuando la capacidad no se tiene en cuenta o no es cumplida dentro de las capacidades de la unidad. | |
| **1–Preliminar** | |
| Contemplado como necesidad, pero no se tienen nada concreto.<br>No existe nada planeado, maneja un ambiente impredecible y reactivo ante las necesidades.<br>Soluciones Ad hoc (solución específicamente para el problema o fin).<br>Al no ser contemplado como una necesidad se encuentra en un estado sin presupuesto.<br>Logran éxitos gracias a esfuerzos heroicos o individuales sin apoyo.<br>Alcanzan el propósito de manera inconsistente, al no ser planeadas, sin seguimiento o medición.<br>El éxito de su empleo no es seguro. | |
| **2–Gestionado** | |
| Planeadas y ejecutadas teniendo en cuenta políticas, procedimientos o normatividad.<br>Para su gestión, el tiempo, costos y recursos son factibles, pero limitados.<br>Es estable y con salidas controladas. | |

De la misma forma se realiza este proceso con todas las variables de las capacidades y subcapacidades a evaluar, obteniendo el resultado deseado por cada capacidad.

## *Operativización del modelo de madurez*

Para la aplicación del modelo es necesario cumplir con el siguiente procedimiento:

- Se debe seleccionar la institución dentro de las fuerzas militares de Colombia a evaluar, sea la Unidad de Cibernética de Comando General, Ejército, Armada Nacional o Fuerza Aérea.
- Se debe definir la misionalidad de la institución a evaluar.
- Tras definir la misionalidad y objetivo de la unidad cibernética, se deben seleccionar las capacidades/subcapacidades que apliquen dentro de cada área funcional del modelo.
- El evaluador se distribuirá con el personal de cada área funcional, ya que dentro de

estas hay funciones y capacidades específicas desempeñadas por la unidad cibernética, obteniendo las respuestas más exactas para el desarrollo del modelo.

- De esta manera se procede a la realización de la evaluación como se expresó en el literal anterior.
- Concluida la evaluación se procede a la verificación de los resultados y aclaración por parte del personal evaluado, si es necesario.
- Posteriormente se realiza la presentación de resultados por capacidad y el plan de trabajo a seguir, de corto, mediano y largo plazo, según la necesidad y urgencia del proceso, teniendo en cuenta la misionalidad de la unidad cibernética.
- El modelo de evaluación deberá ser ejecutado por personal idóneo, con conocimientos en materia cibernética que facilite su aplicación y ejecución de manera más exacta.

Concluyendo, el modelo de madurez aporta los procesos necesarios para el cumplimiento de la misionalidad de la unidad cibernética evaluada y perteneciente a las fuerzas militares, sirviendo como punto de partida para la mejora y ruta de avance en la construcción de capacidades, procesos, toma de decisiones y labores administrativas, de corto, mediano y largo plazo, aportando al buen funcionamiento y desarrollo de la ciberdefensa en cada área funcional de la unidad.

## Discusión

Con la aplicación de este modelo se busca que las unidades cibernéticas de las fuerzas militares tengan las herramientas base y capacidades necesarias para el desarrollo de una buena ciberdefensa, dando una ejecución a procesos de corto, mediano y largo plazo de manera organizada, que ayuda a que las posibles brechas en la defensa y protección sean mínimas.

Así mismo, es necesario tener en cuenta que los objetivos y misionalidades de las unidades cibernéticas pueden ser diferentes, como se aprecia en la tabla 1 y la tabla 6, al ser esenciales o genéricas no aportan una evaluación muy precisa, quedando corta en su ejecución; de esta manera se da cabida a una nueva investigación, dando más granularidad a estas variables que aportaran una mejor decisión en la evaluación y madurez de las capacidades de ciberdefensa.

# Conclusiones

Esta investigación permite concluir que el modelo planteado da respuesta a la problemática presentada, contribuyendo y aportando al alcance de los objetivos de las unidades cibernéticas de las fuerzas militares en el desarrollo y evolución de actividades propias cibernéticas, coadyuvando al progreso y disminución de la brecha digital de la nación de forma segura y confiable; aportando las condiciones necesarias para asistir, de ser necesario, a través de cooperación multilateral, a los países aliados en apoyo a la fuerza cibernética en caso de una ciberguerra, haciendo frente a las ciberamenzas y vulnerabilidades que cada vez son más complejas, destructivas y frecuentes en las condiciones adversas que presenta este quinto dominio de la guerra.

Así mismo, se alude a un futuro trabajo, sugiriendo mejora en las variables según el tipo de proceso u objetivos a evaluar por la unidad cibernética, desagregando más ampliamente cada variable y profundizando en cada nivel de madurez, en referencia a los componentes DOMPI, obteniendo y aportando resultados más detallados y planteando una automatización del modelo.

# Referencias

[Almuhammadi y Alsaleh, 2017] Almuhammadi, S. y Alsaleh, M. (2017). Information Security Maturity. *Computer Science & Information Technology (CS & IT)*. https://www.researchgate.net/profile/Sultan_Almuhammadi/publication/314291503_Information_Security_Maturity_Model_for_Nist_Cyber_Security_Framework/links/5c5e630fa6fdccb608b288de/Information-Security-Maturity-Model-for-Nist-Cyber-Security-\Framework.pdf. ↑Ver página 139

[Arbelaez, 2017] Arbelaez, R. (2017, 21 de febrero). *ACIS VIII Jornada Nacional de Seguridad Informática*. http://52.1.175.72/portal/sites/all/themes/argo/assets/img/Pagina/05-ModelosMadurezSeguridadInformatica.pdf ↑Ver página 134

[Cabuya Padilla y Sierra Abril, 2019] Cabuya Padilla, D.; Sierra Abril, F. (2019). *Método de Evaluación del Sistema Integral de Ciberdefensa-SICID - Reservado*. Bogota: Comando Conjunto Cibernético. ↑Ver página 142, 149, 150

[Comando Conjunto Cibernético, 2018] Comando Conjunto Cibernético. (2018). *Concepto Funciónal Conjunto de Ciberseguridad y Ciberdefensa - Reservado*. Bogota: Comando General de las Fuerzas Militares. ↑Ver página 134, 138

[Departamento Nacional de Planeación, 2021] Departamento Nacional de Planeación. (2021, 14 de julio). Conpes 3701. https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf ↑Ver página 133

[Departamento Nacional de Planeación, 2016] Departamento Nacional de Planeación. (2016, 11 de abril). Conpes 3854 https://bibliotecadigital.ccb.org.co/bitstream/handle/11520/14856/DNP-Conpes-Pol%2b%c2%a1tica%20Nacional%20de%20Seguridad%20Digital.pdf?sequence=1&isAllowed=y ↑Ver página 133

[DOE & Energy, 2014] DOE; Energy, T. U. (2014). *Cybersecurity Capanility Maturity Model (C2M2) Version 1.1.* Carnegie Mellon University. https://www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf ↑Ver página 139

[Goksen, Cevik, & Avunduk, 2015] Goksen, Y.; Cevik, E.; Avunduk, E. (2015). *A Case Analysis On The Focus On The Maturity Models And Information Technologie. Procedia Economics and Finance* (pp. 208-216). Instituto de Tecnología de Tracia, Kavala, Grecia: Elsevier B.V. https://www.sciencedirect.com/science/article/pii/S2212567115000222 ↑Ver página 134, 139

[Junta Interamericana de Defensa, 2020] Junta Interamericana de Defensa; Fundación Interamericana de Defensa. (2020).*Informe II confernecia de Ciberdefensa*. ↑Ver página 134, 138

[Junta Interamericana de Defensa, 2020] Junta Interamericana de Defensa. (2020). *Guia de Ciberdefensa*. Canada: JID. ↑Ver página 134, 138

[Le y Hoang, 2016] Le, N.; Hoang, D. (2016). Can maturity models support cyber? *2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC).* IEEE. https://ieeexplore.ieee.org/document/7820663 ↑Ver página 138, 139

[Villa, Ruiz, & Ramos, 2006] M. Villa, Ruiz, & Ramos. (2006). Un Estudio Crítico Comparativo de ISO 9001, CMMI E ISO 15504. *CISTI Volumen II*, 551. ↑Ver página 140

[OTAN-CCDCOE, 2012] OTAN-CCDCOE. (2012). *National Cyber Security Framework Manual*. Tallinn: Alexander Klimburg. ↑Ver página 134, 138

[Rea-Guamma, Sanchez, Feliu, & Calvo, 2017] Rea-Guamma, A.; Sanchez, I.; Feliu, T.; Calvo, J. (2017). Maturity Models in Cybersecurity: a systematic. *Proceeding of the 12th Iberian Conference on Information Systems and Technologies*, (pp. 284-289). Lisboa, Portugal. https://ieeexplore.ieee.org/document/7975865 ↑Ver página 134, 139

[Villa, Ruiz, & Ramos, 2004] Villa, M.; Ruiz, M.; Ramos, I. (2004). *Modelos de evaluación y mejora de procesos: Análisis comparativo.* https://www.researchgate.net/publication/228925424_Modelos_de_evaluacion_y_mejora_de_procesos_Analisis_comparativo ↑Ver página 140

[White, 2007] White, G. (2007). The Community Cyber Segurity Maturity Model. *Proceeding of the 40th Hawaii International Conference on System Sciences*. ↑Ver página 139