Estrategia para el Fortalecimiento del Plan de Estudios Académico de la "MADGSI", Enfocado desde la Perspectiva de la Ciberseguridad y la Ciberdefensa

Strategy for Strengthening the "Madgsi" Academic Study Plan, Focused from the Perspective of Cyber Security and Cyber-Defense

CT. Robinson Augusto Morales Carvajal, David Enrique López Cortes, Giovanna Estefanía Ramírez Ruíz, Jaquelín Castillo García, Oscar Iván Parra Camacho
Escuela de Postgrados de la Fuerza Aérea Colombiana. Grupo de investigación en Seguridad Integral, Inteligencia y Ciberdefensa (GISIC)
robinson.morales@epfac.edu.co, david.lopez@epfac.edu.co, giovanna.ramirez@epfac.edu.co, jaquelin.castillo@epfac.edu.co, oscar.parra@epfac.edu.co

Este es un artículo de investigación derivado del proyecto titulado "Propuesta de fortalecimiento al Plan de Estudios Académico de la maestría en Dirección y Gestión de la Seguridad Integral (MADGSI)", el cual está enfocado desde la perspectiva de la ciberseguridad y la ciberdefensa al interior de la Escuela de Postgrados de la Fuerza Aérea Colombiana. Dicho proyecto fue realizado por integrantes del grupo de investigación GISIC, con el fin de apoyar el proceso formativo de los estudiantes de la Maestría en Dirección y Gestión de la Seguridad Integral (MADGSI), en la Escuela de Posgrados de la Fuerza Aérea Colombiana, Bogotá, Colombia.

Resumen

El aumento del llamado "ciberespacio" para guardar información importante y confidencial han aumentado la posibilidad de ataques que buscan acceder a la información gubernamental y poner en riesgo sus operaciones. Por eso, se propone la estrategia del fortalecimiento del Plan de Estudios Académico de la maestría en Dirección y Gestión de la Seguridad Integral (MADGSI), enfocada desde la perspectiva de la ciberseguridad y la ciberdefensa al interior de la Escuela de Postgrados de la Fuerza Aérea Colombiana. Ello con el objetivo de facilitar los procesos de investigación y la continua mejora de la capacidad técnica y académica del personal involucrado en el marco del tema a tratar.

Palabras Claves: Amenazas cibernéticas, ciberdefensa, ciberespacio, ciberseguridad, syllabus.

Abstract

The increase in the so-called cyberspace to store important and confidential information has increased the possibility of attacks that pursue to access government information and put their operations at risk. Therefore, the fervent need to implement multiple security measures was created, such as, for example, providing training to officials that receive knowledge and tools to deal with the risks they confront when using digital media. For this reason, the strategy of strengthening the academic curriculum of the master's degree in Direction and Management of Integral Security (MADGSI) is proposed, focused from the perspective of cybersecurity and cyber defense within the Postgraduate School of the Colombian Air Force.

Fecha de Recepción: 23/02/2022 - Aceptado: 01/03/2022 – Publicado: 31/03/2022
ISSN: 2477-9253 – DOI: https://dx.doi.org/10.24133/RCSD.VOL07.N01.2022.05

This was realized with the aim of facilitating the research processes and the continuous improvement of the technical and academic capacity of the personnel involved in the framework of the discussed subject.

Keywords: Cyber defense, cyberspace, cybersecurity, syllabus, computer risk.

I. Introducción

El aumento actual y progresivo del volumen de almacenamiento de datos –junto con la necesidad de mantener información disponible y relevante para el funcionamiento y la toma de decisiones de los Estados– han obligado a las diferentes instituciones públicas a hacer uso del denominado "ciberespacio". Esta coyuntura ha abierto la puerta a continuos y sistematizados ataques que buscan acceder a la información gubernamental y poner en riesgo (o mejor dicho, en peligro) sus operaciones. La situación anterior creó la ferviente necesidad de implementar múltiples medidas de seguridad como, por ejemplo, brindar capacitaciones que provean a los funcionarios de conocimientos y herramientas idóneas para hacer frente a los riesgos que entraña el uso de los medios digitales.

Por todo lo expuesto con anterioridad, se propone la estrategia del fortalecimiento del plan de estudios académico de la Maestría en Dirección y Gestión de la Seguridad Integral (MADGSI), enfocada desde la perspectiva de la ciberseguridad y la ciberdefensa al interior de la Escuela de Postgrados de la Fuerza Aérea Colombiana. Ello en aras de facilitar los procesos de investigación y la continua mejora de la capacidad técnica y académica del personal involucrado en el marco del tema a tratar.

Es así como la maestría en Dirección y Gestión de la Seguridad Integral (MADGSI) es un programa único en Colombia. La oferta curricular de MADGSI parece corresponderse únicamente con las áreas del conocimiento administrativo y de gerencia. Sin embargo, las pretensiones y los esfuerzos del programa están encaminados a enlazar las prácticas profesionales con diferentes disciplinas. Del mismo modo, a pesar de que la maestría nace en una institución educativa militar, la orientación misional pretende incluir también a personal no militar dentro de la apuesta por la seguridad integral, dado que se comprende el carácter multidimensional e interagencial de la seguridad hoy.

II. Justificación

MADGSI fue creada por la Escuela de Postgrados de la Fuerza Aérea Colombiana (EPFAC). El programa académico emerge como una iniciativa de la Fuerza Aérea Colombiana para ampliar las concepciones tanto de la educación como de la seguridad.

Este programa acoge las tendencias y orientaciones de la seguridad integral bajo el entendido mundial de la necesidad de una planificación global que permita el desarrollo de un esquema amplio de investigación e innovación, que facilite la aplicación de variadas metodologías y herramientas para la protección de activos y servicios vitales e infraestructuras críticas en las organizaciones empresariales públicas o privadas, a fin de minimizar las vulnerabilidades, detectar las amenazas y disminuir los factores de riesgo desde la prevención, mediante el empleo de modelos y estándares de gestión nacionales e internacionales.

En la era de la globalización, las amenazas transnacionales se irrigan con facilidad dado que las fronteras entre países son porosas y la convivencia de culturas es internacionalmente más constante; las organizaciones públicas y privadas requieren de un idioma común en materia de seguridad para asegurar que, tanto empresas privadas como Estados, tengan garantía de la protección de sus activos vitales y de la continuidad de sus actividades. La aplicación y generalización del concepto de seguridad integral se reflejaría en mejores prácticas exigidas para los miembros de la industria de la seguridad. De esta manera, las organizaciones nacionales y multinacionales buscan profesionales de la seguridad mejores capacitados, no solamente certificados por organismos internacionales, sino con formación en educación superior que comprenda la complejidad de la seguridad contemporánea.

De esta manera, se percibe que la tendencia actual en la industria de la seguridad es la educación superior, dado que mejorará en la práctica las gestiones y las decisiones de los profesionales de la seguridad dentro del mercado global. Así, los expertos en seguridad con titulación posgradual en diferentes rubros validarán los conocimientos y la experiencia de trabajo. Así mismo, los profesionales de la seguridad con menos experiencia laboral podrán ampliar el campo de acción profesional y garantizarán una comprensión integral de los conceptos y las dinámicas propias de la seguridad integral.

De esta forma, el programa busca la formación integral de un profesional ético, crítico, comprometido y reflexivo. Se resalta a su vez la capacidad del egresado de MADGSI para afrontar resiliente y creativamente los desafíos de seguridad integral; dirigir y gestionar procesos y proyectos en el campo de la seguridad integral, y movilizar procesos de investigación de interés e impacto sobre la seguridad integral. Es así como el programa realiza la actualización curricular en la que se proyectan mejoras sobre el proceso investigativo y sobre la interdisciplinariedad que exige la seguridad integral.

Por esa razón, es necesario avanzar en la investigación y en el desarrollo de las áreas de ciberseguridad y ciberdefensa de la Fuerza Aérea Colombiana, actualizando el pensum de la maestría. Proporcionalmente, también es necesario aumentar el nivel de preparación de los estudiantes y formar gerentes en dichas áreas, ya que el considerable aumento de los ciberataques ha puesto en evidencia la falta de protocolos y respuestas efectivas ante las posibles amenazas que puede llegar a padecer la institución (Monsalve, 2018); ello ha expuesto la vulnerabilidad de sus bancos de información. Por esa razón, se debe fortalecer la estructura curricular académica de la MADGSI y abordar esta nueva línea de investigación en ciberseguridad y ciberdefensa.

El desarrollo de este proyecto permitirá a la Fuerza Aérea Colombiana contar con una mayor preparación y una mejor capacidad de respuesta ante un eventual ciberataque. Además, esta iniciativa pretende fomentar la concientización en materia de seguridad cibernética a través de la formación en ciberseguridad. De esta forma, se expandirá fuera de ámbitos académicos y universitarios, así los futuros profesionales podrán enfrentar y asumir las responsabilidades coyunturales que demandan los sectores públicos y privados de la nación.

III. Metodología

En el desarrollo de este proyecto se usa una metodología basada en la investigación aplicada experimental, debido a que se enlazarán los procesos teóricos y prácticos (existentes) en temas de ciberseguridad al interior de los procesos institucionales de la Fuerza Aérea Colombiana.

Fase 1. Estado del arte

El objetivo de esta fase es recopilar toda la información pertinente mediante una búsqueda sistémica que permita identificar los antecedentes y las metodologías que se vienen aplicando en el marco global y particular de ciberseguridad al interior del sector institucional a tratar. Esta fase se caracteriza por tener un enfoque exploratorio sistémico donde se analizan fuentes de información secundarias. Específicamente: documentos académicos, programas académicos de otras universidades y proyectos similares.

En esta fase se analiza la situación del Plan de Estudios de la maestría y las necesidades que esta tiene, qué materias faltan y pueden ser necesarias para completar el perfil del egresado, así como otras herramientas y medidas de seguridad para hacer frente a los riesgos arraigados a los medios digitales. Por esta razón, se resalta la necesidad e importancia que significa la actualización del pensum para la maestría.

Parte de esta primera sección consistió en hacer un análisis de los otros programas que existen en Colombia. Es así como se llegó a la siguiente información: a nivel nacional, hay ocho programas que comparten contenidos y aproximaciones teóricas similares a MADGSI (Tabla 1). Estos programas de maestría y de especialización se encuentran principalmente en la Universidad Militar Nueva Granada, en la Universidad Externado de Colombia, en la Escuela Superior de Guerra y en la Escuela de Posgrados de la Policía Nacional. Si bien algunos de estos programas contemplan alguna de las temáticas correspondientes con una línea de investigación, solamente MADGSI de la EPFAC realiza el ejercicio de articular de manera amplia y extendida diferentes aspectos de la seguridad pública y privada, en ambos niveles de gestión y de dirección.

Tabla 1: Denominaciones nacionales identificadas por el programa

No	Nivel de formación	Denominación identificada	Número de programas*	Distribución %
1	Maestría	Maestría en Criminología y Victimología	1	12,5%
2	Maestría	Maestría en Seguridad Pública	1	12,5%
3	Especialización	Especialización en Seguridad Integral	1	12,5%
4	Maestría	Maestría en Seguridad y Defensa Nacionales	1	12,5%
5	Maestría	Maestría en Ciberseguridad y Ciberdefensa	1	12,5%
6	Especialización	Especialización en Seguridad y Defensa Nacionales	1	12,5%
7	Maestría	Maestría en Gestión Integral del Riesgo	1	12,5%
8	Especialización	Especialización en Administración de la Seguridad	1	12,5%
Total			8	100%

Esta fase no solo consistió en realizar una investigación bibliográfica de lo que está sucediendo con las instituciones académicas en Colombia, también la maestría, junto con el Departamento de Calidad Académica (DECAE) de la EPFAC, ha realizado dos procesos de autoevaluación en 2019 y 2021, los cuales contemplaron cada una de las condiciones e involucraron cada dependencia de la Escuela y su interacción con MADGSI. Asimismo, los estudiantes, los docentes y los egresados participaron de este proceso y calificaron el cumplimiento de cada condición de calidad y ofrecieron los comentarios correspondientes. Una de las herramientas utilizadas para recoger información fue el de las encuestas. En estas se realizaron preguntas como: "¿Qué tan afines cree que son las líneas de investigación de MADGSI con su propuesta curricular?"; "Como egresado de MADGSI, ¿cree usted que la formación impartida por el programa académico atiende a las necesidades del sector seguridad?"; "De acuerdo con su experiencia, ¿considera que deben incluirse otras materias o módulos? ¿Cuáles?". El informe de autoevaluación de 2019 reporta que los estudiantes sugieren las siguientes acciones: se sugiere realizar una revisión curricular que permita incluir temáticas que estén a la vanguardia de la maestría teniendo en cuenta los rápidos cambios que se presentan en el entorno, de tal forma que los micro currículos incorporen no solo temas locales, sino además internacionales; así mismo vincular en las temáticas a abordar procedimientos, certificaciones y otras formas que utilizan las organizaciones y empresas privadas para realizar la seguridad integral.

Fase 2. Estándares y modelos para la formación en ciberseguridad y ciberdefensa

En esta etapa se busca analizar y comparar los estándares producto de la fase 1, con el fin de identificar cuáles de ellos pueden ser incorporados a los procesos de ciberseguridad en la MADGSI. Esta fase se caracteriza por tener un "enfoque correlacional", ya que este método permite la conexión simbiótica y sinergética entre la información adquirida. De esta forma, se obtendrá un listado de estándares aplicables a los procesos de ciberseguridad en la Fuerza Aérea Colombiana.

Para este proceso es importante conocer las líneas de investigación que articulan la maestría y así ver dónde están las partes que pueden mejorarse. Es así como las Líneas de Investigación de MADGSI con los programas de la FAC se dan desde la función de "Sostener la Fuerza a través del Programa Autonomía Institucional FAC" y se articulan por su objeto de estudio a la Línea Estratégica Seguridad Integral de Instalaciones Vitales Aeronáuticas. A su vez, la Función 'Modernizar la Fuerza con el programa Ventaja Tecnológica' se articula con la línea estratégica Ciberseguridad y Ciberdefensa, como se observa en la Tabla 2:

Tabla 2: Líneas de investigación MADGSI. Grupo de investigación GISIC

Función	Programa FAC	Subprograma	Línea estratégica	Líneas de investigación	Ejes temáticos
Sostener la Fuerza	Autonomía Institucional	Suficiencia Institucional	Seguridad Integral de Instalaciones Vitales Aeronáuticas	Dirección y Gestión de la Seguridad Integral	• Dirección y gestión • Planeación estratégica • Gestión de proyectos • Clima y cultura • Sistemas de gestión • Liderazgo organizacional
				Modelamiento de la Seguridad Integral	• Modelos de seguridad • Gestión del riesgo • Inteligencia • Amenaza transnacional • Protección de infraestructuras críticas • Servicios vitales

Modernizar la Fuerza	Ventaja Tecnológica	Sistemas de Defensa del Ciberespacio	Ciberseguridad y Ciberdefensa	Ciberseguridad y Ciberdefensa	• Inteligencia artificial • Criptografía • Blockchain • Internet de las cosas • Contenido malicioso • Dispositivo Móvil

Como bien se ve en la tabla, la tercera línea de investigación se desprende de la función de la FAC 'Modernizar la Fuerza' y de la línea estratégica 'Ciberseguridad y Ciberdefensa'. La importancia del ciberespacio para la FAC es creciente dado que, en las últimas normatividades, como la Estrategia 2042, se considera que la misionalidad de la institución se debe extender hacia la conquista del espacio digital. En la actualidad no sería posible considerar la seguridad integral sin el ciberespacio; las tecnologías de la información y de las comunicaciones han sido esenciales en el avance de la globalización. Por ello, la ciberseguridad se convierte en una necesidad urgente para su estudio y aplicación.

El objetivo de la creación de la línea de investigación en ciberseguridad y ciberdefensa es el fomento de la cultura de ciberseguridad para que los directores y gestores de la seguridad integral adopten dentro de su práctica profesional la protección de la información digital. La ciberseguridad tiene una estrecha relación con conocimientos específicos en informática e ingeniería, pero también tiene implicaciones sobre la política, la economía y la cultura. Las temáticas que encierra la ciberseguridad como el Blockchain, la criptografía o la inteligencia artificial están en constante interacción con las personas a través de las redes sociales, las transferencias bancarias y los virus informáticos. Es más, la seguridad de la infraestructura física no es concebible actualmente sin la seguridad informática debido a la tecnología y a la informática aplicada a dispositivos de seguridad.

Si bien Internet existe desde hace cuarenta años, la aplicabilidad a la vida cotidiana es exclusivamente del siglo XXI. Por este motivo, la regulación y la protección de las actividades en línea son de reciente data. La convergencia de diferentes tipos de criminalidad internacional hoy hace que la explotación de los medios informáticos sea indispensable (Matfess & Miklaucic, 2016). En consecuencia, los Estados y las empresas han debido desarrollar sistemas de seguridad y de defensa informática que proteja a las personas y a las organizaciones. Esta línea de investigación propende hacia el desarrollo de mecanismos que mitiguen las vulnerabilidades en este espacio.

Estas consideraciones deben incluirse dentro del modelamiento o la dirección/gestión de la seguridad integral en tanto las interacciones humanas hoy dependen necesariamente de la mediación de los aparatos electrónicos, softwares, inteligencia artificial, aplicaciones y conexiones a internet; la exposición que sufren las personas y las organizaciones requieren de una profundización en los estudios de seguridad para buscar soluciones innovadoras y reducir los riesgos de captura de datos o de estafa. La ciberseguridad es trasversal a la vida del ser humano contemporáneo y articula tanto la seguridad como el riesgo y la amenaza, y debe tratarse tanto en el campo virtual como en las costumbres y las prácticas de los usuarios. El estudio de la ciberseguridad se extendería entonces a los usos de las tecnologías de la información tanto en la vida cotidiana como en las operaciones de las organizaciones estatales y privadas.

Fase 3. Creación de una malla curricular para la línea de ciberseguridad de la MADGSI

El objetivo de esta fase es integrar los resultados obtenidos en las fases 1 y 2. Esto con el fin de crear un syllabus que se adapte a la maestría en Desarrollo y Gestión de la Seguridad Integral (MADGSI) de la FAC (Fuerza Aérea Colombiana) y que cumpla con las debidas prácticas en gerencia e investigación de la ciberseguridad y la ciberdefensa. A partir de ello, será factible la obtención de una adecuada formación de los estudiantes en materia de ciberseguridad.

En las figuras 1 y 2 se indican los módulos de la maestría que se relacionan con la línea de investigación Ciberseguridad y Ciberdefensa. En el núcleo de ciberseguridad se encuentra el módulo 'Fundamento de seguridad y ciberdefensa' y en la electivas está el módulo 'Seguridad en el ciberespacio'. Allí la competencia central es la protección de la información dado que los contenidos se enfocan en el fomento de la cultura de la ciberseguridad, a partir de la identificación de los procesos de conectividad entre usuarios, empresas y Estados, y de algunos procesos técnicos donde ocurren las mayores vulnerabilidades del ciberespacio para cualquier comunicación o transacción.

CIBERSEGURIDAD Y CIBERDEFENSA	FUNDAMENTOS DE CIBERSEGURIDAD Y CIBERDEFENSA		
	24	72	2

Figura 1: Núcleos de ciberseguridad y ciberdefensa del currículo de MADGSI

ELECTIVAS		
SEGURIDAD Y SALUD EN EL TRABAJO		
24	72	2
SEGURIDAD AEROPORTUARIA		
24	72	2
SEGURIDAD EN EL CIBERESPACIO		
24	72	2

Figura 2: Núcleos de electivas del currículo de MADGSI
Nota. Elaboración propia. El color naranja corresponde a la intensidad horaria con acompañamiento directo, el blanco es intensidad horaria-trabajo independiente y el amarillo el número de créditos.

Fase 4. Integración de la malla curricular al plan académico de la maestría

Después de crear la nueva malla curricular de la maestría se debe incorporar al programa, más específicamente a la línea de investigación de ciberseguridad y ciberdefensa. Es así como toda esta investigación que se realizó en las fases anteriores ayudará a mejorar el documento maestro del programa de maestría. Así como dar inicio con las nuevas clases y cumplir con los objetivos propuestos en cada una de ellas.

Fase 5. Trabajo futuro

El objetivo de esta etapa es crear un laboratorio físico dentro del cual se llevarán a cabo las prácticas y experimentos de ciberseguridad, los cuales están relacionados con la malla curricular mencionada anteriormente. A partir de la creación de dicho espacio, surgirán las siguientes necesidades: adquirir planos del laboratorio; adecuar la infraestructura (es decir: el salón de la EPFAC); comprar equipos de cómputo e instrumentos del laboratorio y realizar pruebas de los equipos. Todo ello será la base material que proveerá el apropiado funcionamiento del laboratorio. De esta manera se podrá implementar y validar la malla curricular elaborada.

IV. Evaluación de Resultados y Discusión

Como parte de toda la investigación que se realizó para la creación de este curso, se creó el syllabus, es decir, las clases que le van a dar continuidad al programa. A continuación, se explicarán cada uno de los módulos que integrarán dicho programa. Todo esto con el fin de proporcionar las herramientas necesarias para que el estudiante aprenda de primera mano las habilidades necesarias para la ciberseguridad y la ciberdefensa.

Syllabus: fundamentos de la ciberseguridad y la ciberdefensa

Este módulo es de gran pertinencia, ya que brinda las herramientas necesarias para que el estudiante conozca, interprete y aplique los conocimientos de la ciberseguridad relacionados con la seguridad integral. Ello, posiblemente, le permitirá generar habilidades y destrezas para la protección de la información y desempeñarse con eficacia dentro del marco investigativo que la seguridad exige, e incentivar iniciativas o propuestas en materia de ciberseguridad para cubrir riesgos y amenazas del sector.

El estudiante, al finalizar la asignatura, estará en la capacidad de identificar riesgos y vulnerabilidades que se pueden presentar en el campo de la seguridad informática. De igual forma, podrá analizar, interpretar y correlacionar todos aquellos modelos, protocolos y técnicas pertenecientes al campo de la ciberseguridad; con el fin de aplicarlos al contexto real de la protección de la información.

El estudio y la aplicación de la seguridad informática, enfocada a la ciberseguridad y ciberdefensa, es fundamental dentro del ámbito gerencial y laboral, ya que permitirá desempeñar distintos perfiles profesionales en distintos entornos de aplicación. Además, también se exigiría con suma rigurosidad que los actores tengan los conocimientos adecuados y conducentes para que sus labores sean implementadas de acuerdo con los marcos legales que exige la ley.

Las competencias que desarrollará el estudiante son la cognitiva, la procedimental, la actitudinal y la investigativa. Todo esto para definir, interpretar y aplicar las teorías y conceptos de la ciberseguridad y la ciberdefensa en el contexto de la seguridad informática.

Este tiene 4 unidades: 1) Introducción a la ciberseguridad y la ciberdefensa. En esta se tratan los temas de ciberespacio y hacking ético. 2) Ciberataques. El footprinting y vectores de ataque. 3) Ciberseguridad en la ingeniería social. En esta unidad se trabaja lo que es la ingeniería social. 4) Normatividad y legislación en la ciberseguridad. Aquí se trabaja la informática forense. Cada una de estas unidades cuenta con unos temas y una evaluación final.

Por otra parte, cada una de las unidades temáticas tienen unos criterios de evaluación. Las evaluaciones tendrán un propósito formativo y serán de carácter: 1) Cuantitativo: cuando a la evaluación correspondiente se le asigne una calificación de carácter numérico para medir el rendimiento del estudiante. 2) Cualitativa: es aquella donde se juzga o valora más la calidad tanto del proceso como el nivel de aprovechamiento de las herramientas frente al diseño del sistema integrado de gestión.

La evaluación se concibe como un proceso que busca medir el dominio y aplicación de conceptos referentes a la ciberseguridad y la ciberdefensa del área de la seguridad informática por parte del estudiante, identificando el nivel de progreso e interiorización de la gestión por procesos en procura del cumplimiento de requisitos establecidos para el producto o servicio del proceso estudiado, con el fin de que el educando pueda alcanzar los resultados o logros de aprendizaje deseados. Dentro de los principales mecanismos de evaluación establecidos en el Modelo Pedagógico Holístico Castrense Aeronáutico 2017 (pp. 32-34), en el programa se conciben las siguientes:

a. Prueba de conocimiento oral y escrita

b. Exposiciones

c. Trabajos escritos

d. Talleres

e. Laboratorios

f. Pre-informes

g. Informes

h. Casos de estudio

i. Proyectos

j. Simulaciones

k. Solución de problemas

Para los módulos aplican tres actividades evaluativas que generarán tres cortes con la siguiente ponderación: primer corte 30 %, segundo corte 30 % y tercer corte 40 %, para un consolidado del 100 % de la calificación final del módulo. La agrupación de trabajos y demás actividades para generar las notas anteriormente descritas, están a criterio del docente y su presentación debe contener dos decimales.

La asistencia a las actividades evaluativas prácticas y/o en grupo (exposiciones y/o sustentaciones, talleres, entre otros) es de carácter obligatorio y la inasistencia a una de ellas será calificada con 0.00 (cero, punto, cero cero).

Syllabus electivo: seguridad en el ciberespacio

Este módulo brindará las herramientas necesarias para que el estudiante interprete y aplique los conocimientos de la seguridad en el ciberespacio; permitiéndole así generar habilidades y destrezas que contribuyan a la protección de la información y al desempeño adecuado dentro del marco investigativo que la seguridad exige. Además, dicho modulo también le permitirá proyectar iniciativas y propuestas en materia de ciberseguridad necesarias para combatir los riesgos que amenazan a la institución.

Este tiene 4 unidades: 1) Reconocimiento de sistemas informáticos: en esta unidad se ven los temas de footprinting y escaneo. 2) Vectores de ataque: se tratan los temas de ataques criptográficos, ataques a redes Wi-fi, ataques web, intrusión física e ingeniería social. 3) Informática forense: informática forense. 4) Ethical Hacking: hacking ético.

V. Conclusiones y Trabajo Futuro

El fortalecimiento del plan de estudios de la MADGSI traerá distintas ventajas para la formación de los estudiantes de la maestría, ya que les dará un panorama más amplio de lo que es la seguridad. Especialmente, si se considera que el desarrollo del mundo digital es la principal tendencia de la contemporaneidad. Dicha coyuntura, ha hecho que los ataques cibernéticos sean más frecuentes cada día, y por dicha razón, la Fuerza Aérea Colombiana debe tener las herramientas adecuadas para combatir los ciberataques; así como proporcionar ayuda a las otras entidades del Estado o privadas.

Referencias

Cano, J. (2011). *Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto globa*l. Sistemas (asociación colombiana de ingenieros de sistemas), 119(4.7).

Escuela de posgrados. Fuerza Aérea Colombiana. (2021). *Descripción y fundamentación epistemológica de las líneas de investigación MAGDASI*. Escuela de Posgrados de la Fuerza Aérea Colombiana.

Escuela de posgrados. Fuerza Aérea Colombiana. (2020). *Documento Maestro. Maestría en Dirección de y Gestión de la Seguridad Integral.* Escuela de Posgrados de la Fuerza Aérea Colombiana.

Escuela de posgrados. Fuerza Aérea Colombiana. (2021). *Informe de la evaluación del proyecto educativo del programa*. Escuela de Posgrados de la Fuerza Aérea Colombiana.

Fernández Bermejo, D., & Martínez Atienza, G. (2018). *Ciberseguridad, ciberespacio y ciberdelincuencia* (pp. 1-236). Thomson Reuters Aranzadi.

Fuerza Aérea Colombiana. (2014). Legislación Educativa - *Sistema Educativo de la Fuerza Aérea Colombiana.* Colombia: imprenta y publicaciones FUERZAS MILITARES REPÚBLICA DE COLOMBIA.

Fuerza Aérea Colombiana. (2020). *Documentos Maestro de la Maestría en Dirección y Gestión de la Seguridad Integral*. DOCUMENTO MAESTRO MADGSI-EPFAC-Resaltado[3623].pdf

Gutarra Meza, F. N. (2021). Sílabo de Seguridad de la información corporativa.

Matfess, H. & Miklaucic, M. (2016). *Beyond convergence*. World without order. National Defense University Press.

Monsalve Méndez, J. Y. (2018). Ciberseguridad: principales amenazas en Colombia (ingeniería social, Phishing y Dos).

Rico Venegas, Y., López Cortés, D. E. y Cerón Rincón, A. (2020). Enfoques y gestión en Seguridad Integral. Escuela de posgrados Fuerza Aérea Colombiana. https://doi.org/10.18667/9789585996199

Villanueva Méndez, J. C. (2015). La ciberdefensa en Colombia (Bachelor's thesis, Universidad Piloto de Colombia)

Zambrano, S. M. Q., & Valencia, D. G. M. (2017). Seguridad en informática: consideraciones. Dominio de las Ciencias, 3(3), 676-688.