DIPLOMATURA UNIVERSITARIA

“Gestión de la Ciberdefensa”

INICIO VÍA Google Meet

PRESENCIAL SEGÚN EVOLUCIÓN DE LA PANDEMIA.

PLAN CURRICULAR

UNDEF

FMC

DIPLOMATURA UNIVERSITARIA EN GESTIÓN DE LA CIBERDEFENSA AÑO 2021

1. ANTECEDENTES:

La cuestión ciberespacial implica una de las problemáticas de mayor actualidad y cada día incorpora más actividades y acciones al quehacer diario del ser humano.

Este nuevo ambiente de desarrollo de la actividad humana que en el siglo XXI ha crecido y continúa haciéndolo de manera exponencial, de la mano de las tecnologías de la información y las comunicaciones (TICs), encuentra a la mayoría de los habitantes en un cierto nivel de desprotección acerca de cómo desenvolverse, cuáles son los peligros que en él acechan y cuáles son las medidas que permiten desarrollar confianza en sí mismo.

Desde el punto de vista estratégico que nos ocupa se convoca a un nuevo ambiente operacional, donde los estados en función de sus intereses y particularidades de sus habitantes, intentan buscar diferentes formas de dominio del mismo y sus fuerzas armadas y de seguridad, desarrollar nuevas operaciones de características especialmente originales

2. JUSTIFICACIÓN GENERAL:

Moverse en el ciberespacio es el desafío más agobiante de la modernidad; su gestión y el conocimiento de procesos y procedimientos, resultan esenciales al hombre moderno en general, ya que en este ambiente se desarrollan desde actividades lúdicas y recetas de cocina hasta el diseño de los más sofisticado sistemas, pasando por las estrategias nacionales, el desarrollo de refinadas formas ataques cibernéticos de alta rentabilidad, activismo hacker y de ciberdefensa militar, científica e industrial, todo está en la nube, va por las redes o lo que es peor, sobre los sistemas de control y telecomando de procesos, todo se desarrolla en lo que llamamos ciberespacio.

Conocer el ciberespacio y las actividades que en él se desarrollan, es probablemente un desafío que enfrenta el hombre moderno llamado a gestionar organizaciones, empresas, sociedades o casi cualquier actividad humana, incluso en el nivel de la "Internet de las Cosas".

En una clara comprensión de esta problemática la escuela Superior de Guerra Conjunta de las Fuerza Armadas, inició en 2017 el proyecto de Vigilancia Tecnológica: "Observatorio Argentino del Ciberespacio", financiado a través de proyectos UNDEFI, hasta el año 2018; el objetivo del mismo es llevar al conocimiento de la comunidad educativa en particular y a la sociedad en general, noticias y aspectos que son propios de este nuevo ambiente del desarrollo de los conflictos humanos.

Para atender la necesidad de promover capacitación para el gerenciamiento de aspectos relacionados con la Ciberdefensa, se ha trabajado sobre un enfoque metodológico, conceptual y funcionalmente interdisciplinario que ha dado como resultado el conjunto de metodologías didácticas que permiten acercar conocimientos necesarios para quienes debe gestionar e interactuar en diferentes organizaciones, empresas o dominios.

3. OBJETIVOS:

a. OBJETIVO GENERAL

La diplomatura en Gestión de la Ciberdefensa ofrece una oferta académica que abarca la introducción a la cuestión ciberespacial y su problemática, para profundizar luego en el gerenciamiento de la Ciberdefensa a través de contenidos teóricos, ejercitaciones prácticas y un núcleo de conferencias de reconocidos expertos en el tema.

b. OBJETIVOS ESPECÍFICOS

- Presentar los aspectos generales de Ciberdefensa y su relación con la Tecnología de la Información.
- Complementar la formación de cuadros gerenciales en el ámbito de la Ciberdefensa, enfocada al Planeamiento Estratégico en el área, y la formación y entrenamiento de los Recursos Humanos comprometidos ante conflictos entre estados naciones.
- Destacar la importancia extrema de la ética en los equipos que actúen enfrentando, episodios Ciber Bélicos entre estados naciones.
- Estudiar los aspectos jurídicos a ser tenidos en cuenta por quienes actúen enfrentando situaciones mencionadas en el párrafo anterior.
- Preparar a los participantes para formar parte de los denominados equipos CERT (Computer Emergency Response Team) y para su desempeño en posiciones de liderazgo en diversos tipos de emprendimientos en el campo de la ciberdefensa.
- Introducir a los alumnos en el gerenciamiento en las Infraestructuras Críticas, la Ciberdisuasión y los principios, normas y sistemas de Gestión - COBIT, ITIL e ISO 27000, mediante el análisis de casos prácticos de teoría de juegos aplicada al ambiente del ciberconflicto.

4. PERFILES A LOS QUE SE DIRIGE LA DIPLOMATURA:

La diplomatura está dirigida a funcionarios de la administración pública y del ámbito privado con posiciones de liderazgo, y personas con interés en los aspectos vinculados a la Defensa Nacional en general, y en la ciberdefensa en particular.

5. DURACIÓN Y MODALIDAD DE DICTADO

- 30 jornadas a dictarse los días martes y jueves de 18:00 a 21.00 HS

- Total: 90 horas

- Modalidad presencial. Inicio vía Google Meet, y posteriormente según evolución de la situación provocada por la pandemia.

6. MODALIDAD DE TRABAJO:

Se concretará mediante la integración de equipos multidisciplinarios con la finalidad de lograr la vivencia del trabajo que caracteriza fundamentalmente al área de gerenciamiento de los ciberconflictos.

7. PAUTAS GENERALES DE APROBACIÓN:

Los alumnos deberán:

- Haber asistido al 75% de las clases.
- Haber aprobado la práctica profesional (Ejercicio Final), grupal interdisciplinario.
- Haber participado del Debate de Consolidación Final o bien presentar un Ensayo Académico Breve en el Debate de Consolidación (A criterio del Director de Diplomatura).
- Haber concretado un trabajo integrador grupal / individual final. (Ensayo Académico Breve -3000 a 4000 palabras-, con su visión aplicada de algunas de las áreas del ciberespacio).

8. PROGRAMA SINTÉTICO DE LA DIPLOMATURA. MÉTODO DE DESARROLLO DE LAS CLASES:

La estrategia metodológica esencial estará orientada al estudio de casos. Se incluirán exposiciones individuales.

El 70% de la carga horaria estará dedicada a aspectos conceptuales y el otro 30% a aspectos práctico / instrumentales. Estos últimos, se materializarán mediante el desarrollo de tres Casos Prácticos:

- Caso 1: Análisis del “Caso Snowden”.

a. Recopilación y análisis de antecedentes
b. Estimación de los daños causados a los EEUU por el “Caso Snowden”
c. ¿Cuáles fueron las vulnerabilidades de distinto tipo evidenciadas por el “Caso Snowden?
d. Situación actual y estimación de la evolución probable del “Caso Snowden”.

- Caso 2: Análisis del “Caso Assange”.

a. Recopilación y análisis de antecedentes de Julián Assange y de WikiLeaks
b. Estimación de los daños causados por WikiLeaks ¿Afectados por WikiLeaks?
c. ¿Cuáles fueron las vulnerabilidades de distinto tipo evidenció WikiLeaks?
d. Situación actual y estimación de la evolución probable de la situación de Julián Assange.

- Caso 3: Evaluación de la viabilidad de adaptación del Tallin Manual a la Región

a. Recopilación de antecedentes del Tallin Manual (versión actual).
b. Análisis de los puntos de vista del líder del equipo que elaboró el Tallin Manual (versión actual), Profesor Michael N. Schmitt Ph.D. (análisis de los videos generados por el CCDCOE al respecto).
c. Coincidencias y divergencias entre el Tallin Manual (versión actual) y la letra y el espíritu del Artículo 51 de la Carta de las Naciones Unidas. Coincidencias y divergencias entre el Tallin Manual y la doctrina vigente en la Región en los aspectos correspondientes del Derecho Internacional Público.

ÁREA EL CIBERESPACIO AMBIENTE OPERACIONAL

MÓDULO 1: Ciberespacio y ambiente operacional I

Duración: 6hs

Docentes Titulares: Brigadier Mayor (R) Mg. Alejandro Moresi

Licenciado Hugo Miguel

- Relación entre Ambientes Operacionales y el Ciberespacio.
- El Factor Humano en los Ciber Conflictos.
- Análisis comparativo del peso que el Factor Humanos tuvo en distintos casos de Ciber Conflictos.
- Las Armas y el Ciberespacio.
- Análisis de las arquitecturas de Ciber Armas que se han utilizado en los episodios / conflictos más resonantes.
- Análisis de los Sistemas de Detección de Intrusiones que se utilizaron en distintos casos de Ciber Conflictos.

MÓDULO 02: Ciberespacio y ambiente operacional II

Duración: 6hs

Docente Titular: Teniente Coronel OIM (R) Carlos Federico Amaya

- Espectro Electromagnético y Ciberespacio. ¿Qué es, cómo se emplea? el espectro electromagnético, descripción de amenazas sobre el mismo.
- De lo analógico a lo digital. Actividades ofensivas, la inhibición de emisiones. Concepción de un sistema de transmisión de información
- La guerra electrónica de comunicaciones y de no comunicaciones
- Estructura OSI. La ciberdefensa en la Argentina, estado actual. De UKUSA al convenio de Budapest.

MÓDULO 03: Historia y análisis de conflictos

Duración: 3hs

Docente Titular: Brigadier Mayor (R) Mg. Alejandro Moresi

- Historia Casos y la situación legal: Ciber Conflictos y Derecho Internacional. Aspectos forenses más relevantes asociados a los Ciber Conflictos. El manual de Tallin.
- Estudio de casos: Caso Snowden, Caso Assange.
- La situación Legal del ciberespacio en Argentina: organizaciones, legislación, la situación actual y las limitaciones que produce.

MÓDULO 04: OPERACIONES EN EL CIBERESPACIO

Duración: 3hs
Docente Titular: Lic. Hugo Miguel

- Las operaciones Ciberespaciales: Operaciones Ofensivas, defensivas y de exploración. La diferencias entre Ciberseguridad y Ciberdefensa, concepto de infraestructuras críticas. Matrices de solución de problemas de Ciberdefensa.
- Ética y Ciber Conflictos. Análisis de casos reales en los que sea evidente la preponderancia de la ética en los equipos y en las personas actuantes en Ciber Conflictos. Estudio de casos en los que los aspectos éticos evidencien su rol preponderante en los Ciber Conflictos
- Descripción y análisis de incidentes / agresiones que hayan constituido acciones resonantes entre estados naciones. Descripción y análisis de las herramientas de Tecnología Informática asociados

ÁREA INFORMACIÓN Y CIBERESPACIO

MÓDULO 01: OPERACIONES DE INFORMACIÓN

Duración: 2hs
Docente Titular: General de División (R) Evergisto De Vergara

- El rol de la información como instrumento del poder nacional en la consecución de los objetivos estratégicos militares.

- Los principios, capacidades y limitaciones de las operaciones de información en el conflicto contemporáneo.
- La integración de las operaciones de información y las operaciones en el entorno de información.

<u>MÓDULO 02</u>: RECURSOS HUMANOS

Duración: 1h
Docente Titular: Dr. Guillermo Rutz

Los RRHH en los diferentes niveles: ¿Qué necesito, de donde lo obtengo y como capacito al RRHH de nivel estratégico, operacional y táctico.

ÁREA GESTIÓN DE LA CIBERDEFENSA

<u>MÓDULO 01</u>: INTRODUCCIÓN AL GERENCIAMIENTO INNOVADOR

Duración: 6hs
Docente Titular: CL (R) Gabriel Urchipia
Docente Invitado: Lic. Susana García

- La capacidad emprendedora en las organizaciones.
- Los procesos de gestión del conocimiento.
- Dinámicas de Innovación y creatividad: la innovación en la Cuarta Revolución Industrial, la creatividad en la fusión de nuevas tecnologías.
- La Gestión de Proyectos en empresas de desarrollo tecnológico.
- La Gestión de Calidad en las soluciones tecnológicas aplicadas a la ciberdefensa y ciberseguridad.
- La familia de estándares ISO 27000. Cuadros de mando integral como herramienta de gestión frente a las amenazas y desafíos cibernéticos.

<u>MÓDULO 02</u>: INTRODUCCIÓN A LA CRIPTOLOGÍA

Duración: 3hs
Docente Titular: Mayor (R) FA Mg. Jorge Eterovic
Docente Invitado: Lic. Marcelo Cipriano

- Los primeros sistemas criptográficos en tiempos de griegos y romanos.
- Los aportes de la Teoría de la Información, la Matemática Discreta, la Teoría de los Grandes Números y los aportes de la Ciencia de la Computación
- Criptografía simétrica. Criptografía asimétrica. Criptografía Visual

MÓDULO 03: TECNOLOGÍA DE REDES

Duración: 6hs
Docente Titular: Capitán de Corbeta Ingeniero Jorge Ríos
Docente Invitado: Dra. Antonieta Kuz

- Introducción a las redes de datos.
- Señales analógicas y digitales. Modulación
- Topologías en bus, anillo y estrella.
- Conmutación de circuitos y paquetes
  - Protocolo Ethernet. CSMA/CD. Ethernet sobre cable de cobre. Ethernet sobre fibra óptica
  - Protocolos TCP, UDP, IP versiones
  - Arquitectura de las redes WAN. PSTN
  - Arquitectura de la red Internet

MÓDULO 04: PLANEAMIENTO ESTRATÉGICO DE LA CIBERDEFENSA

Duración: 6hs
Docente Titular: Brigadier Mayor (R) Mg. Alejandro Moresi

- Características de los Ciber Ataques Masivos a Sistemas de Información. Estudio de las alternativas para la detección de las primeras fases del Ciber Ataque

- Ciber Ataques Masivos del tipo Denegación Distribuida de Servicios (DDoS). Arquitectura de un esquema DDoS.
- Respuesta ante Ciber Ataques Masivos. Analisis de casos en el ámbito de la Ciberdefensa .
- Principios y Sistemas de Gestión de la Ciberdefensa .
- Respuesta “preventiva” (Ciber disuasión).
- La Metodología COBIT (Control Objectives for Information and related Technology)
- COBIT 5, sus principios y terminología. Aportes potenciales de COBIT 5 en Ciberdefensa y Ciberseguridad. Arquitectura de productos COBIT 5. Los 5 principios de COBIT 5 aplicados en Ciberdefensa y Ciberseguridad. Los procesos de COBIT 5 y el Modelo de Referencia de Procesos (PRM). Ciclo de vida de la Implantación de Procesos y de la Gestión

MÓDULO 05: GERENCIAMIENTO DE LA CIBERDEFENSA EN INFRAESTRUCTURAS CRÍTICAS – DISEÑOS DE ESCENARIOS Y ESTRATEGIAS EN EL CIBERESPACIO

Duración: 15hs
Docente Titular: Contraalmirante (R) Gabriel Urchipia.

- De la metafísica a la cibernética, evolución en la concepción del rol de la tecnología en la sociedad.
- El abordaje sistémico de los riesgos y el abordaje integral de los riesgos cibernéticos.
- Diagnóstico, teoría y práctica de la estrategia.
- Práctica de la estrategia (Inteligencia, análisis de la situación)
- Evolución, evaluación, apreciación, resolución y supervisión.
- Teoría de juegos aplicadas al diagnóstico de escenarios. Agresiones, intromisiones cometidos en el dominio cibernético.
- Planeamiento estratégico en contextos competitivos.
- El empleo de estrategias como proceso cibernético y de auto aprendizaje.

MÓDULO 06: GERENCIAMIENTO DE LA CIBERDEFENSA EN INFRAESTRUCTURAS CRÍTICAS

Duración: 3hs

Docente Titular: Dr. Nicolás Tato

Dra. Viviana Petracini

- Principios y Sistemas de Gestión de la Ciberdefensa.
- Principios generales del Derecho Internacional aplicables en el Ciberespacio.
- Integridad Internacional: Desafíos en el Ciberespacio. No-Intervención en un Ciber Contexto. Ciberespacio: Obligaciones del Estado en el Área de Derechos Humanos. Regulaciones internacionales en el ámbito de las Comunicaciones. Ciber Actividades violatorias del Derecho Internacional

BIBLIOTECA DE INFRAESTRUCTURA DE TECNOLOGÍA DE LA INFORMACIÓN (ITIL)

Duración: 3hs

Docente Titular: Coronel (R) OIM Juan José Benítez

- La Biblioteca de Infraestructura de Tecnologías de Información (ITIL): como un conjunto de conceptos y buenas prácticas de gestión de las Tecnologías de la Información.
- Aportes posibles de ITIL en Ciberdefensa. ITIL como conjunto de procedimientos de Gestión de la Tecnología de la Información.
- ISO/IEC 27000 - Vocabulario estándar para el SGSI.
- ISO/IEC 27001 – Requisitos para certificar.
- ISO/IEC 27002 – Buenas prácticas.
- ISO/IEC 27003 - Directrices para la implementación de un SGSI.
- ISO/IEC 27004 - Métricas para la gestión de seguridad de la información.
- ISO/IEC 27005 - Gestión de riesgos en seguridad de la información.

CICLO DE CONFERENCIAS

1. Ciberespacio, el nacimiento de un nuevo objetivo.
   Expositor invitado: BM (R) Mg. Alejandro Moresi

2. Operaciones de Información – Pericias forenses.
   Expositor Invitado: Ing. Manrique González Avellaneda

3. El Comando Conjunto de Ciberdefensa
   Expositor Invitado: GB Aníbal Intini.

4. La Dirección de Ciberdefensa de la Fuerza Aérea Argentina y de la Armada de la República Argentina.
   Expositor Invitado: CN Daniel Sorrentino
   Expositor Invitado: A determinar por FAA.

5. El rol del estado en el desarrollo de TICs.
   Expositor Invitado: Lic. Hugo Darío Miguel

6. Las operaciones Ciberespaciales: Operaciones ofensivas, defensivas y de exploración. La diferencia entre Ciberseguridad y Ciberdefensa, concepto de infraestructuras críticas. Matrices de solución de problemas de Ciberdefensa
   Expositor Invitado: Dr. Alejandro Corletti

7. Ciberataques en la nube de conmutación de canales.
   Expositor Invitado: Mg. Daniel Perles
   Ciberseguridad de infraestructuras en centrales termonucleares
   Expositor Invitado: Ing. Julián Di Cesare

8. La Argentina y la cuarta revolución industrial
   Expositor Invitado: Brigadier Mayor (R) Mg. Alejandro Moresi

BIBLIOGRAFÍA:

a. BIBLIOGRAFÍA BÁSICA

- NATO “Peacetime Regime for State Activities in Cyberspace” CCDCOE, 2013. https://ccdcoe.org/multimedia/peacetime-regime-state-activities-cyberspace.html
- Clarke, Richard A., Knake, Roberto K., “Cyber War”, Harper Collins, 2002
- NATO “Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations to Be Launched”, CCDCOE, 2017 https://ccdcoe.org/tallinn-manual-20-international-law-applicable-cyber-operations-be-launched.html
- Uzal, Roberto, “Guerra Cibernética. ¿un desafío para la Defensa Nacional?, Visón Conjunta (Revista de la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas de Argentina), Año 4, Nro. 7. 2012
- Cyber Operatios Joint Publication 3-12, Jun 2018 https://fas.org/irp/doddir/dod/jp3_12.pdf http://www.esgcffaa.edu.ar/pdf/ESGCFFAA-2016_pdf-33.pdf (página 40)
- Irán Hoy - Guerra cibernética contra Irán – YouTube (Video de la Televisión de Irán). https://www.youtube.com/watch?v=vrRj-kRofRg
- Uzal, Roberto. et al “Ciber Lavado Transnacional de Activos” publicado, referato mediante, en los anales de las 44 Jornadas Argentinas de Informática e Investigación Operativa. SADIO, 2015. http://44jaiio.sadio.org.ar/sites/default/files/sie160-179.pdf
- Uzal, Roberto, “El Problema de la Ciber Atribución. Aportes para una Estrategia de Ciberdefensa”. Consejo Argentino para las Relaciones Internacionales, septiembre 2015 http://www.cari.org.ar/pdf/boletin61.pdf
- Uzal, Roberto, “Ciber Ius ad bellum”: Aportes para definir las reglas de empeñamiento militar de Argentina y de otros países de la Región en los casos de Ciber-Conflictos entre estados naciones, Consejo Argentino para las Relaciones Internacionales, noviembre 2015. http://www.cari.org.ar/pdf/boletin62.pdf
- Uzal, Roberto, “Ciberdefensa: El Factor Crítico de Éxito Esencial”, Consejo Argentino para las Relaciones Internacionales, abril 2016. http://www.cari.org.ar/pdf/boletin63.pdf

b. BIBLIOGRAFIA COMPLEMENTARIA

- Uzal, Roberto, “Ciber Disuasión: Un capítulo particularmente sensitivo de la Ciberdefensa”, Consejo Argentino para las Relaciones Internacionales, Julio 2016 http://www.cari.org.ar/pdf/boletin64.pdf
- Uzal, Roberto, “Ciber Califato y Ciber Hezbollah: Consideraciones y propuestas”, Consejo Argentino para las Relaciones Internacionales, marzo 2017 http://www.cari.org.ar/pdf/boletin65.pdf
- Uzal, Roberto, Amaya, Carlos, Apuntes / Transparencias de la asignatura “Tecnología de la Información, ética y normativa jurídica”, FCE-UBA, octubre / noviembre 2017
- Rousseff, Dilma, “Discurso ante la Asamblea de las Naciones Unidas”, 2013 https://www.youtube.com/watch?v=nz0V2qsPrt0
- Stone, Oliver, “Snowden” (Película) https://www.nytimes.com/2016/09/16/movies/snowden-review-oliver-stone-joseph-gordon-levitt.html
- Scarano, Eduardo, “Manual de redacción de escritos de investigación”, Editorial: Macchi Grupo Editor, I.S.B.N: 950537612X, 2004 http://ciece.com.ar/ciece/wp-content/uploads/Manual%20de%20Redaccion%20de%20Escritos%20de%20Investigacion2.pdf