Universidad Nacional
de San Luis

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

BORRADOR PRELIMINAR DE LA ESTRUCTURA Y FUNDAMENTOS DE LA MAESTRIA EN CIBERDEFENSA Y EN CIBERSEGURIDAD

Fundamentos del proyecto de elaboración de la Maestría en Ciberdefensa y Ciberseguridad con las orientaciones aspectos operativos de Ciberdefensa y de Ciberseguridad y aspectos forenses de Ciberdefensa y de Ciberseguridad

1. Necesidad de contar, en nuestro país y en la región, con Recursos Humanos altamente calificados para actuar ante agresiones en el Ciberespacio que afecten la Infraestructura Crítica del país o aspectos esenciales de la Soberanía Nacional (Ciber Espionaje) y también para actuar en casos de actos delictivos de alto nivel de sofisticación que también se llevan a cabo, ay con cierta habitualidad, en el Ciberespacio.
2. Necesidad de que nuestras Fuerzas Armadas estén capacitadas para actuar cuando Fuerzas Armadas extranjeras actúen contra nuestro país en el nuevo dominio de los conflictos entre estados naciones: El Ciberespacio
3. Necesidad de profesionales altamente capacitados para actuar cuando nuestro sistema de salud, nuestro sistema de seguridad social, nuestro sistema financiero u otros sistemas de similar sensibilidad, sean objeto de sofisticadas Ciber Agresiones provenientes desde el exterior o desde el interior de nuestro país.
4. Necesidad de que, las corporaciones empresariales cuya actuación sea de alta sensibilidad para la economía y/o sectores sociales de nuestro país, cuenten con profesionales altamente capacitados para actuar ante potenciales o reales Ciber Agresiones que puedan afectar la continuidad de sus operaciones
5. Necesidad de que nuestras Fuerzas de Seguridad y Fuerzas Policiales cuenten con personal altamente capacitados para actuar ante esquemas delictivos sofisticados que se verifican en el Ciberespacio tal como el Ciber Lavado Transnacional de Activos y otros de similar gravedad.
6. Conveniencia de ajustar, en los contenidos y orientación de la Maestría en Ciberdefensa y Ciberseguridad a los “estándares de facto” que han venido consensuándose en los últimos años.
7. Conveniencia de que el desarrollo de los módulos de la Maestría en Ciberdefensa y Ciberseguridad esté a cargo de académicos internacionalmente reconocidos, con una adecuada

categorización científica y con conocimientos y experiencias objetivamente reconocidos.

Título a otorgarse:

Magister en Ciberdefensa y en Ciberseguridad

Orientaciones:

- **Aspectos operativos de Ciberdefensa y de Ciberseguridad**
- **Aspectos forenses de Ciberdefensa y de Ciberseguridad**

Carga total horaria total:

580 horas de cursos correspondientes a 29 créditos
160 horas de investigación supervisada y/o tutoriales
Tesis de Maestría

Duración:

2 años

Requisitos para el ingreso:

Graduado en estudios universitarios correspondientes a carreras oficialmente reconocidas de la República Argentina y del exterior de cuatro o más años de duración.

REFERENCIA *CONTENIDOS DEFINIDOS POR LA NATO*

http://www.ttu.ee/studying/masters/masters_programmes/cyber-security/

Ciberdefensa y Ciberseguridad

Proteger a la Infraestructura Crítica de un país (energía, transporte, comunicaciones, sistema financiero, salud, previsión social, sistemas de información del Gobierno y de las Fuerzas Armadas) constituye el desafío más relevante de la Defensa Nacional. Desde hace algo menos de una década, las Ciber Agresiones han sido las más insidiosas y peligrosas causales de riesgo de los componentes de la citada Infraestructura Crítica en diversos países. La prevención de estas agresiones y la actuación en caso de producirse constituyen las incumbencias esenciales de la Ciberdefensa.

Sabemos que el Ciber Espionaje, por otro lado, ha devenido en una de las manifestaciones más contundentes de violación de la soberanía de diversos

estados naciones. Evitar o por lo menos mitigar este tipo de Ciber Agresión constituye otro desafío insoslayable.

Por otro lado, el demorar la preparación para prevenir y actuar adecuadamente ante actos de Ciber Terrorismo constituye una grave carencia de la Gestión Gubernamental.

En paralelo a lo ya destacado, en el ámbito Corporativo - Empresarial, las Ciber Agresiones han venido manifestándose de maneras igualmente graves y sofisticadas; se han manifestado en forma análoga a lo ocurrido en las Ciber Agresiones entre estados naciones.

Ciber Espionaje, Ciber Terrorismo, sofisticadas Ciber Agresiones a Corporaciones Empresariales constituyen, junto a otras muy complejas formas delictivas en el Ciberespacio, las incumbencias típicas de la Ciberseguridad.

Ciberdefensa y Ciberseguridad, necesariamente, deben ser aspectos de especial interés en las universidades, tanto en lo que hace a formación del cuarto nivel como en el contexto de las actividades de Investigación y Desarrollo

Es por ello que la Universidad Nacional de San Luis, ampliamente reconocida a nivel nacional e internacional en los distintos ámbitos de la Tecnología Informática, Ingeniería del Software, Calidad del Software y en el de las diversas manifestaciones de las Ciencias de la Computación, ofrece esta Maestría en Ciberdefensa y en Ciberseguridad con dos orientaciones: a) “Aspectos operativos de Ciberdefensa y de Ciberseguridad” y b) “Aspectos forenses de Ciberdefensa y de Ciberseguridad”.

Este Programa de Maestría suministra a sus alumnos amplios conocimientos y habilidades adecuadas en el ámbito de la seguridad de los Sistemas de Información, tanto a nivel gubernamental como en el ámbito empresarial. También abarca aspectos vinculados a incidentes de seguridad cibernética y actividades relacionadas con la actividad forense en el Ciberespacio. Los alumnos de la Maestría tendrán la oportunidad de entrenarse con expertos de primer nivel nacional, regional e internacional; entre dichos expertos participarán especialistas en aspectos militares vinculados al Ciberespacio, ejecutivos bancarios, expertos del ámbito de las telecomunicaciones, expertos del ámbito policial de la Ciberseguridad, del entorno judicial e integrantes experimentados de CERTs (Computer Emergencies Response Teams) entre otras personalidades reconocidas en Ciberdefensa y en Ciberseguridad.

El programa de Maestría está pensado teniendo en cuenta experiencias similares en Europa en general y en la Organización del Tratado de Atlántico Norte en particular y también en los actuales convenios de co tutela con universidades de Europa y de Brasil. Por otro lado se ha tenido especialmente en cuenta la posible futura continuación de los estudios en el contexto de los doctorados que se desarrollan en la Facultad de Ciencias Físico-Matemáticas y Naturales de la UNSL.

Aspectos claves

- Se trata de un programa de Maestría que es único en el país; en el mismo se ha volcado el know how de docentes con experiencia concreta en el tema y que gozan de amplio reconocimiento nacional y regional.
- Se trata de un programa desarrollado en un ámbito en el cual la UNSL posee experiencia exitosa reconocida a nivel nacional e internacional.
- Se trabajará en una muy estrecha colaboración con integrantes de equipos de Ciberdefensa y de Ciberseguridad de nuestro país y de países amigos.

CURRÍCULA SINTÉTICA DE LAS ORIENTACIONES:

- Magister en Ciberdefensa y en Ciberseguridad Orientación "Aspectos operativos de Ciberdefensa y de Ciberseguridad"

Es de público conocimiento que los estados naciones deben enfrentar, en forma claramente creciente, Ciber Agresiones a su Infraestructura Crítica y actos de Ciber Espionaje masivo provenientes mayoritariamente, en los dos casos mencionados, desde otros estados naciones. Por otro lado, ante la no vigencia de tratados específicos, la única posibilidad de respuesta a las Ciber Agresiones y al Ciber Espionaje es el ejercicio del derecho que surge de los contenidos del Artículo 51 de la Carta de las Naciones Unidas. Lo expresado hasta aquí, en este párrafo, constituyen las claras incumbencias de la Ciberdefensa. En forma análoga a los estados naciones, organizaciones de todo tipo y también individuos, han sido y están siendo objeto de Ciber Agresiones de un nivel de sofisticación llamativo. Ciber Delincuentes y Ciber Terroristas han demostrado contar con Ciber Armas y Ciber Arquitecturas de un nivel de complejidad análogo al de las utilizadas por los estados naciones pioneros en este contexto. Ciber Delitos y Ciber Terrorismo son típicas incumbencias de la Ciberseguridad. Los especialistas en Ciberseguridad deben prevenir acciones ilícitas en el Ciberespacio, detectar la ejecución de Ciber Delitos y de actos de Ciber Terrorismo para lo cual deben contar con capacidades para detectar los orígenes de los mismos y herramientas para interrumpir la ejecución de actividades que claramente violan la ley y que se ejecuten, como se señaló, en el Ciberespacio.

- Magister en Ciberdefensa y en Ciberseguridad Orientación "Aspectos forenses de Ciberdefensa y de Ciberseguridad"

Experiencias repetidas y contundentes muestran que los estados naciones deben contar con capacidad forense creíble y deseablemente homologada tal que les permitan, cuando fuere necesario, concurrir con sólidos elementos de prueba, ante organismos internacionales, a efectos de denunciar a estados naciones Ciber Agresores. Algo análogo ocurre en el caso de Ciber Delitos y Ciber Terrorismo; los organismos de Ciberseguridad deben contar con las capacidades de producción de pruebas que permitan llevar ante los tribunales

correspondientes, nacionales e inclusive internacionales, a los responsables de violar la ley en el Ciberespacio.

CURRÍCULA SINTÉTICA DE LAS ORIENTACIONES:

Estructura del Curriculum de las dos orientaciones de la Maestría:

1. Cursos de formación general: 4 créditos
2. Cursos fundamentales de Ciberdefensa y Ciberseguridad: 9 créditos
3. Cursos especiales de Ciberdefensa y Ciberseguridad: 13 créditos (existen múltiples opciones)
4. Cursos de libre elección: 3 créditos
5. Investigación Supervisada y/o Tutoriales: 8 créditos
6. Tesis de Maestría

a) Título a ser otorgado:

- Magister en Ciberdefensa y en Ciberseguridad Orientación "Aspectos operativos de Ciberdefensa y de Ciberseguridad"

a.1. MÓDULO: Cursos de formación general: 4 créditos

Objetivo:
El objetivo general de este módulo es el de alcanzar un nivel adecuado de formación general nivelada en los alumnos graduados mediante la transmisión de conocimientos y habilidades en los aspectos débiles del perfil del alumno
.
Resultados del aprendizaje:
Luego de haber aprobado la totalidad de este módulo el alumno debe haber adquirido:
- Conocimientos básicos de gerenciamiento de la innovación (entrepreneurship)
- Capacidad de análisis y utilización de principios éticos en el desempeño profesional en Ciberdefensa y Ciberseguridad
- Nivelación en aquellas áreas de conocimiento / habilidades en las que el alumno evidencie debilidades al iniciar la Maestría.

a.1.1. Materias Obligatorias: 2 créditos

a.1.1.1. Tecnología de la Información, ética y normativa jurídica: 1 crédito
a.1.1.2. Introducción al gerenciamiento innovador (entrepreneurship): 1 crédito

a.1.2. Materias Optativas: 2 créditos

a.1.2.1. Tecno-psicología: 1 crédito
a.1.2.2. Innovación y resolución creativa de problemas: 1 crédito
a.1.2.3. Introducción a la Programación: 1 crédito
a.1.2.4. Introducción a la Tecnología de la Información: 1 crédito
a.1.2.5. Informática Social: 1 crédito
a.1.2.6. Introducción a la Psicología de Internet: 1 crédito

a.2. MÓDULO: Cursos fundamentales de Ciberdefensa y Ciberseguridad: 9 créditos

a.2.1. Cursos fundamentales de Ciberdefensa y Ciberseguridad (Estudios Básicos): 3 créditos

Objetivo:
Crear la "base de sustentación" para el desarrollo de los cursos subsiguientes.

Resultados del aprendizaje:
A través del cursado de este módulo el alumno adquirirá:

- Conocimientos básicos relacionados con operaciones militares en el Ciberespacio y los primeros aspectos vinculados a Ciberdefensa
- Conocimientos jurídicos básicos para encarar aspectos relacionados con Ciberseguridad entendida como la prevención y represión de acciones delictivas en el Ciberespacio
- Conocimientos básicos de Criptología

a.2.1.1. Aspectos legales de la Ciberseguridad: 1 crédito
(Derecho penal, Derecho Internacional, seguridad de la Información, teleinformática, cooperación internacional en Ciberseguridad, conceptos y terminología)
a.2.1.2. Introducción a la Criptología: 1 crédito
(Algoritmos Criptográficos, Técnicas Cripto Analíticas, Sistemas Crptográficos, Sistema RSA, Firma Digital, Funciones Hash)
a.2.1.3. Evolución de la Tecnología Militar hasta el enfoque “Network-Centric Warfare”: 1 crédito
(Evolución del “Arte de la Guerra”. El rol del Ciberespacio en la conducción militar moderna)

a.2.2. Cursos fundamentales de Ciberdefensa y Ciberseguridad (Estudios fundamentales): 6 créditos

Objetivo:
Suministrar los conocimientos fundamentales de Ciberdefensa y de Ciberseguridad a la totalidad de los alumnos

Resultados del aprendizaje:
- Acceder a los conocimientos fundamentales de Redes de Computadoras
- Contar con una visión general de las amenazas y ataques a Sistemas de Información
- Acceder a los conocimientos necesarios para gerenciar la Seguridad Informática y para gerenciar los incidentes derivados de Ciber Ataques.

a.2.2.1. Tecnología de Redes: 2 créditos
a.2.2.2. Malware: 1 crédito
(Worms, trojans, rootkits, botnets. Detección temprana)
a.2.2.3. Fundamentos y Gerenciameinto de la Ciberdefensa y de la Ciberseguridad: 2 créditos
(Ciberdefensa y Ciberseguridad – Fundamentos – Principios y Sistemas de Gestión - COBIT, ITIL, ISO 27000)
a.2.2.4. Ciber Ataques masivos a Sistemas de Información – La Defensa ante Ciber Ataques – Roles de la Ciberdefensa y de la Ciberseguridad: 1 crédito
(Métodos y estrategias de Ciberdefensa y de Ciberseguridad, trabajo de equipo en Ciberdefensa y en Ciberseguridad)

a.3. MÓDULO: Cursos especiales de Ciberdefensa y Ciberseguridad: 13 créditos (existen múltiples opciones)

Objetivo:
Posibilitar al alumno una cierta especialización en el área general de la Ciberdefensa y de la Ciberseguridad. Los cursos están, en general, clasificados como cursos de tecnología, de gestión y de criptología. Los alumnos tienen la posibilidad de seleccionar un conjunto de cursos que se correspondan con su área de interés.

Resultados del aprendizaje:
- Adquirir una sólida especialización / competencia en los aspectos seleccionados de acuerdo con el perfil elegido por el alumno.
- Adquirir experiencia en aspectos instrumentales en diversas tecnologías relacionadas con la Ciberdefensa y con la Ciberseguridad.
- Evaluar los distintos enfoques metodológicos de Ciberdefensa y de Ciberseguridad de manera de estar en condiciones de desarrollar la Estrategia de Ciberdefensa o de Ciberseguridad más adecuada en un determinado escenario.

a.3.1. Materias Obligatorias: 3 créditos

a.3.1.1. Seminario de Ciberdefensa: 1 crédito
a.3.1.2. Principios y enfoques de Diseño de Software Seguro: 1 crédito (Balance entre requerimientos funcionales y no funcionales, detección de fallas, recuperación, integridad, validación y verificación)
a.3.1.3. Principios y enfoques de Diseño de Software Seguro. Desarrollo de un Proyecto: 1 crédito

a.3.2. Materias Optativas: 10 créditos

a.3.2.1. Teoría Organizacional y Psicología Organizacional: 2 créditos
a.3.2.2. Diseño y Desarrollo de la “Data Exchange Layer” en ambientes de Gobierno: 2 créditos
a.3.2.3. Sistemas de Información: 2 créditos
a.3.2.4. Data Mining y Análisis de Redes: 2 créditos (Análisis cuali cuantitativo, detección de fraudes, análisis de redes)
a.3.2.5. Tecnología de Redes II: 2 créditos
a.3.2.6. Seguridad en Redes de Computadoras: 2 créditos
a.3.2.7. Curso Especial de Ciberdefensa y Ciberseguridad: 1 crédito
a.3.2.8. Malware II: 1 crédito
a.3.2.9. Hacking: Ataques y defensa de Sistemas de Información: 1 crédito
a.3.2.10. Soluciones para el Monitoreo de Ciberdefensa y Ciberseguridad: 2 créditos
a.3.2.11. Simulación de Ataques y Defensa en Ciberdefensa y en Ciberseguridad: 2 créditos
a.3.2.12. Aseguramiento de la Ciberseguridad en distintos tipos de Organizaciones: 2 créditos
a.3.2.13. Entrenamiento mediante Casos Prácticos: 2 créditos
a.3.2.14. Criptología I: 2 créditos
a.3.2.15. Criptología II: 2 créditos
a.3.2.16. Protocolos Criptográficos: 2 créditos

a.3.2.17. Técnicas de Programación Segura: 1 crédito
a.3.2.18. Técnicas de Programación Segura. Proyecto: 1 crédito
a.3.2.19. Criptografía aplicada: 2 créditos
a.3.2.20. Seminario de Investigación en Criptografía: 2 créditos
a.3.2.21. Tópicos Especiales en Criptografía: 1 crédito
a.3.2.22. Tecnología de Redes II: 2 créditos
a.3.2.23. Administración de Sistemas en contextos de Ciberdefensa y Ciberseguridad: 2 créditos

a.4. MÓDULO: Cursos de libre elección: 3 créditos

Objetivo:
Posibilitar que el alumno pueda, libremente, elegir cursos que él estime interesantes y útiles.

Resultados del aprendizaje:
Que el alumno pueda explicar cómo aplicar a la Ciberdefensa y a la Ciberseguridad los conocimientos adquiridos en los cursos de libre elección studies.

a.5. Investigación Supervisada y/o Tutoriales: 8 créditos

Actividades de investigación supervisada y/o tutoriales, con un mínimo de 8 créditos, independientemente de las horas que demande la Tesis.

a.6. Tesis de Maestría

Objetivo:
- Desarrollar los conocimientos y habilidades adquiridos
- Obtener experiencia en la solución de problemas de Ciberdefensa y Ciberseguridad mediante un aporte relevante a la disciplina

Resultados del aprendizaje:
- Consolidar, profundizar y ampliar el conocimiento profesional del alumno mediante un aporte creativo e innovador.

b) Título a ser otorgado:

- **Magister en Ciberdefensa y en Ciberseguridad Orientación "Aspectos forenses de Ciberdefensa y de Ciberseguridad"**

b.1. MÓDULO: Cursos de formación general: 4 créditos

Objetivo:
El objetivo general de este módulo es el de alcanzar un nivel adecuado de formación general nivelada en los alumnos graduados mediante la transmisión de conocimientos y habilidades en los aspectos débiles del perfil del alumno
.
Resultados del aprendizaje:
Luego de haber aprobado la totalidad de este módulo el alumno debe haber adquirido:
- Conocimientos básicos de gerenciamiento de la innovación (entrepreneurship)
- Capacidad de análisis y utilización de principios éticos en el desempeño profesional en Ciberdefensa y Ciberseguridad
- Nivelación en aquellas áreas de conocimiento / habilidades en las que el alumno evidencie debilidades al iniciar la Maestría.

b.1.1. Materias Obligatorias: 2 créditos

b.1.1.1. Tecnología de la Información, ética y normativa jurídica: 1 crédito
b.1.1.2. Introducción al gerenciamiento innovador (entrepreneurship): 1 crédito

b.1.2. Materias Optativas: 2 créditos

b.1.2.1. Tecno-psicología: 1 crédito
b.1.2.2. Innovación y resolución creativa de problemas: 1 crédito
b.1.2.3. Introducción a la Programación: 1 crédito
b.1.2.4. Introducción a la Tecnología de la Información: 1 crédito
b.1.2.5. Informática social: 1 crédito
b.1.2.6. Introducción a la Psicología de Internet: 1crédito

b.2. MÓDULO: Cursos fundamentales de Ciberdefensa y Ciberseguridad: 9 créditos

b.2.1. Tópicos de Informática Jurídica e Informática Forense (Aspectos Básicos): 3 créditos

Objetivo:
Suministrar conocimientos básicos de Informática Jurídica e Informática Forense

Resultados del aprendizaje:
Una vez que este módulo haya sido desarrollado, el alumno tendrá:

- Una visión básica de los aspectos normativos relacionados con la privacidad, protección de datos personales y libertad de la información
- Un adecuado conocimiento de la elaboración de la "evidencia digital" y la recolección y preservación de dicha "evidencia digital"
- Una visión general de los sistemas operativos de uso en la actualidad desde un punto de vista de la obtención, recolección y guarda de la "evidencia digital".

b.2.1.1. Normas jurídicas sobre privacidad y protección de datos: 1 crédito (Privacidad, derecho de acceso a la información, autoridades con incumbencias en la protección de datos)
b.2.1.2. Una visión general de los sistemas operativos y software de base en general, de uso en la actual, desde un punto de vista de la obtención, recolección y guarda de la "evidencia digital": 1 crédito
b.2.1.3. Naturaleza y aspectos instrumentales de Evidencia y Prueba Digital: 1 crédito

b.2.2. Tópicos de Informática Jurídica e Informática Forense (Aspectos Avanzados): 6 créditos

Objetivo:
Suministrar con la profundidad adecuada los conocimientos sobre Informática Jurídica e Informática Forense a los alumnos de esta orientación.

Resultados del aprendizaje:
- La labor forense en Redes de Computadoras
- La labor forense en casos de amenazas y ataques a los sistemas de información
- La labor forense en el manejo de la seguridad y en la gestión de incidentes en sistemas de información.

b.2.2.1. Tecnología de Redes con un enfoque forense I: 2 créditos
b.2.2.2. Malware y aspectos forenses relacionados: 1 crédito (Worms, trojans, rootkits, botnets. Detección temprana, consideraciones forenses)
b.2.2.3. Fundamentos y Gestión de la Ciberdefensa y la Ciberseguridad: Un enfoque forense: 2 créditos (Ciberdefensa y Ciberseguridad, fundamentos, métodos de gestión y principios aplicables, COBIT, ITIL, ISO 27000)
b.2.2.4. Ataques masivos a sistemas de información y métodos defensivos desde un enfoque forense: 1 crédito (Métodos y estrategias de protección de sistemas de información desde un punto de vista forense, trabajo en equipo en la protección de sistemas de información)

b.3. MÓDULO: Cursos especiales de Ciberdefensa y Ciberseguridad: 13 créditos (existen múltiples opciones)

Objetivo:
Posibilitar al alumno una cierta especialización dentro del enfoque general de la Informática Forense. El alumno podrá seleccionar cursos de acuerdo con sus intereses y necesidades.

Resultados del aprendizaje:
- Adquisición de una cierta especialización y obtención de competencias de acuerdo con el perfil profesional que se desea alcanzar.

b.3.1. Materias Obligatorias: 4 créditos

b.3.1.1. Informática forense y sistemas de información: 1 crédito
(Recolección de evidencias a partir de "vuelcos" de memoria, análisis de dispositivos, estudio de archivos y registros, estudio de los "logs" de transacciones, creación y análisis de "bitácoras" (audit trail)
b.3.1.2. Informática forense en Redes Complejas: 1 crédito
(Análisis de Datos de Redes, IPS, IDS, Automatización del Análisis de Datos de Redes, estudio de protocolos de redes)
b.3.1.3. Métodos para el manejo de incidentes: Informática Forense en el Ciberespacio: 1 crédito
(Incidentes de Ciber Seguridad, Procedimientos de Gestión de Incidentes, puntos de vista de Ciberdefensa y de Ciberseguridad)
b.3.1.4. Seminario de Informática Forense: 1 crédito
(Peculiaridades, aseguramiento, y colección de evidencia digital en diferentes jurisdicciones)

b.3.2. Materias Optativas: 9 créditos

b.3.2.1. Derechos, Obligaciones y Responsabilidades de los Actores en Internet: 1 crédito
b.3.2.2. Data Mining y Análisis de Redes: 2 créditos
(Análisis cuali cuantitativo, detección automatizada de fraudes, Análisis de Redes)
b.3.2.3. Tecnología de Redes con un enfoque forense II: 2 créditos
b.3.2.4. Seguridad en las Redes de Computadoras: 2 créditos
b.3.2.5. Malware II: 1 crédito
b.3.2.6. Hacking de Sistemas de Información: Ataque y Defensa: 1 crédito
b.3.2.7. Soluciones de Monitoreo de Ciberdefensa: 2 créditos
b.2.1.8. Introducción a la Teoría de los Números, Análisis Combinatorio y Criptografía Elemental: 1 crédito
b.2.1.9. Curso Especial de Informática Forense I: 1 crédito
b.2.1.10. Curso Especial de Informática Forense II: 1 crédito
b.2.1.11. Práctica de Campo de Informática Forense: 2 créditos
b.3.2.12. Criptología I: 2 créditos
b.3.2.13. Criptografía Aplicada: 2 créditos

b.4. MÓDULO: Cursos de libre elección: 3 créditos

Objetivo:
Posibilitar que el alumno pueda, libremente, elegir cursos que él estime interesantes y útiles.

Resultados del aprendizaje:
Que el alumno pueda explicar cómo aplicar a los aspectos forenses de la Ciberdefensa y de la Ciberseguridad los conocimientos adquiridos en los cursos de libre elección studies.

b.5. Investigación Supervisada o Tutoriales: 8 créditos

Actividades de investigación supervisada y/o tutoriales, con un mínimo de 8 créditos, independientemente de las horas que demande la Tesis.

b.6. Tesis de Maestría

Objetivo:
- Desarrollar los conocimientos y habilidades adquiridos
- Obtener experiencia en la solución de problemas de Ciberdefensa y Ciberseguridad mediante un aporte relevante a la disciplina

Resultados del aprendizaje:
- Consolidar, profundizar y ampliar el conocimiento profesional del alumno mediante un aporte creativo e innovador.