Newman
Escuela de Posgrado

Plan de Estudio 2023

Maestría en Ciberseguridad

Programa de Maestría

1. Maestría en Ciberseguridad (+) (*) (**)

La Maestría en Ciberseguridad en su modalidad a distancia se desarrolla a través del siguiente plan de estudios:

Cod.	Asignatura	HT	HP	CR
101 – MC	Ciberdelitos y Regulación de la Ciberseguridad	80	0	5
102 – MC	Gobierno de la Ciberseguridad y Análisis de Riesgos	80	0	5
103 – MC	Seguridad en Redes y Análisis Inteligente de Amenazas	80	0	5
104 – MC	Informática Forense y Respuesta ante Incidentes	80	0	5
105 – MC	Metodología de la Investigación I	64	0	4
201 – MC	Seguridad en Sistemas, Aplicaciones y Datos Masivos	80	0	5
202 – MC	Desarrollo Seguro de Software y Auditoría de la Ciberseguridad	80	0	5
203 – MC	Acceso Ético a Sistemas y Análisis de Programas Malignos	80	0	5
204 – MC	Mecanismos Criptográficos, de Autenticación y Control de Acceso	80	0	5
205 – MC	Metodología de la Investigación II	64	0	4
	Total horas y créditos curriculares	**768**		**48**

Adicionalmente al programa de estudios oficial, de forma complementaria la Escuela de Posgrado Newman brinda la oportunidad a sus estudiantes de ampliar sus conocimientos y profundizar en temáticas de interés relacionadas a su especialidad, con la finalidad de potenciar y cumplir con el perfil del egresado deseado y a su vez aporte valor a su desarrollo profesional por medio de competencias específicas. Se debe considerar que, estos créditos complementarios no condicionan la emisión del grado, ni incorporan alguna denominación o mención adicional a la que tiene aprobada la Escuela:

Créditos complementarios (***)						
N°	**Curso de Especialización en Metodologías Ágiles**	**HT**	**HP**	**CR**	**CRX**	**CRC**
301	Design Thinking	64	0	0	0	4
302	Estrategia Lean	64	0	0	0	4
303	Scrum	64	0	0	0	4
	Total de horas y créditos complementarios	**192**				**12**
N°	**Curso de Especialización en Dirección de Proyectos**	**HT**	**HP**	**CR**	**CRX**	**CRC**
401	Gestión de las adquisiciones y los interesados	64	0	0	0	4
402	Integración y alcance de proyectos	64	0	0	0	4
403	Gestión de las comunicaciones y del riesgo	64	0	0	0	4
	Total de horas y créditos complementarios	**192**				**12**

HT: Horas teóricas
HP: Horas prácticas
CR: Créditos curriculares
Horas Curriculares: 768
CC: Créditos complementarios
(+) Maestría de especialización
(*) Campo del Conocimiento UNESCO: 6. Tecnologías de la Información y la Comunicación
(**) Campo de Investigación OCDE: 2.00.00 Ingeniería y Tecnología
(***) Créditos complementarios que no condicionan la emisión del grado, ni modifican la denominación del grado oficial.

Asignaturas con créditos obligatorios: 101, 102, 103, 104, 105, 201, 202, 203, 204 y 205
Asignaturas con créditos complementarios no obligatorios: 301, 302, 303, 401, 402 y 403

1.1. Sumilla del Plan de Estudio

Las sumillas de las asignaturas son las siguientes:

Código 101 – MC
Ciberdelitos y Regulación de la Ciberseguridad

Al término de la asignatura, el estudiante aplicará los conocimientos legales necesarios, tanto terminológicos como sustantivos, para manejar apropiadamente los conceptos y la terminología legal, así como la normativa vigente en materia de ciberdelitos y ciberseguridad.

Agregado a lo anterior, categorizará temas relativos a la protección de datos, al Esquema Nacional de Seguridad, a los servicios de la sociedad de la información y al comerico electrónico, la tipología de delitos informáticos, los fraudes en la red y en medios de pago y los ataques de malware diverso para analizar su funcionamiento y evaluar su impacto.

Por otro lado, conocerá las distintas técnicas utilizadas por la ciberdelincuencia como paso previo del aprendizaje a su mitigación. Así, diferenciará técnicas de ataque a través de spam, ransomware o botnets, que afectan diariamente a miles de dispositivos y las tendencias en ataques de ingeniería social.

Código 102 – MC
Gobierno de la Ciberseguridad y Análisis de Riesgos

Al término de la asignatura, el estudiante empleará los conocimientos fundamentales acerca del gobierno de la seguridad de la información, así como los estándares, modelos de buenas prácticas de gestión y de madurez en el área de la seguridad de la información.

Asimismo, identificará las certificaciones fundamentales en el área de la seguridad de la información y los procesos de certificación, así como los aspectos económicos, con el objetivo de resaltar que la seguridad es un proceso continuo de mejora y no un estado de un sistema, por lo que las políticas y controles establecidos para la protección de la información deberán revisarse, probarse y adecuarse, de ser necesario, ante los nuevos riesgos que se identifiquen.

Código 103 – MC
Seguridad en Redes y Análisis Inteligente de Amenazas

Al término de la asignatura, el estudiante describirá las tecnologías de protección de los sistemas de información distribuidos, así como en las vulnerabilidades y amenazas de los sistemas de información en red para posteriormente en contraposición presentar los protocolos de seguridad más habituales para su protección.

En ese sentido, experimentarán con las topologías de protección de los sistemas basados en cortafuegos y en la protección proactiva de los sistemas con el objetivo de utilizar las estrategias de protección basadas en señuelos, sistemas de detección y protección de intrusión y los sistemas gestores de eventos de seguridad (SIEM aspectos de mayor actualidad, ya que este tipo de salvaguardas son la principal protección para las amenazas activas persistentes (denominadas APT, Advanced Persistent Threat).

Además, inspeccionará los conceptos fundamentales de la criptografía aplicada a la seguridad en redes como algoritmos de cifrado simétrico y asimétrico, firma digital, autenticación de mensajes y funciones resumen para proponer protocolos seguros tanto en redes cableadas (MACsec, IPSec, SSL/TLS y DNSsec) como en redes inalámbricas (WEP, WPA, WPA2 y WPA3).

Código 104 – MC
Informática Forense y Respuesta ante Incidentes

Al término de la asignatura, el estudiante aplicará los conocimientos técnicos y legales en el campo de la respuesta a incidentes y del análisis forense digital, a través de una investigación práctica que concluya con la confección de un informe pericial sobre la misma.

Además, gestionará y organizará la propia información obtenida para enfrentarse a los distintos tipos de incidentes y análisis, logrando integrar la capacidad técnica, los conocimientos y la experiencia en la extracción de datos, el análisis y la presentación de pruebas para un uso legal como especialista en el ámbito.

Código 105 – MC
Metodología de la Investigación I

La asignatura tiene como propósito fortalecer en los estudiantes las competencias sobre métodos y técnicas de investigación a través de los siguientes contenidos académicos: el trabajo de investigación, modalidades de trabajo de investigación, estructura del trabajo de investigación estructura del plan, el título del tema y el planteamiento del problema.

Código 201 – MC
Seguridad en Sistemas, Aplicaciones y Datos Masivos

Al término de la asignatura, el estudiante implementará la seguridad de sistemas operativos y de las aplicaciones web para que una vez desplegadas online, se comporten de la forma esperada, tanto por los propietarios como por parte de los usuarios de la aplicación y puedan mitigar cualquier ataque.

Además, profundizará en la seguridad de los servicios desplegados de arquitecturas en la nube y de big data, antes y una vez desplegados los sistemas y aplicaciones evaluando el Ciclo de Vida de Desarrollo Seguro de Software (SSCLC): los requisitos de seguridad, el diseño y desarrollo seguros, así como las pruebas y operaciones de seguridad que se deben llevar a cabo de forma ordenada y procedimental por personal experto en seguridad.

Código 202 – MC
Desarrollo Seguro de Software y Auditoría de la Ciberseguridad

Al término de la asignatura, el estudiante practicará los principios de diseño de seguridad, las principales técnicas de protección frente a ataques y amenazas en el software de aplicación, así como el concepto de vulnerabilidad, su tipología y el análisis de vulnerabilidad de una aplicación.

Además, utilizará los lenguajes de programación y herramientas de auditoría de código fuente desde el punto de vista de la seguridad informática y, realizará auditorías de seguridad que permitan conocer el estado de la seguridad de la organización y promover acciones de mejora, así como los principales estándares, metodologías, herramientas y buenas prácticas de auditoría de la seguridad con la finalidad de analizar, con vistas a las eventuales acciones correctivas, la seguridad y los controles internos que tiene implantados una organización para garantizar la integridad, disponibilidad y confidencialidad de sus servicios y la información que manejan.

Incluso, propondrá la necesidad de incluir en las organizaciones un proceso sistemático o disciplina que aborde la seguridad en todas las etapas del ciclo de vida de desarrollo del software que incluya una serie de buenas prácticas de seguridad (S-SDLC) como especificación, requisitos de seguridad, casos de abuso, análisis de riesgo, análisis de código, pruebas de penetración dinámicas, modelado de amenazas, operaciones de seguridad y revisiones externas necesarias para asegurar la confianza y robustez del mismo, para conseguir un software confiable.

Código 203 – MC
Acceso Ético a Sistemas y Análisis de Programas Malignos

Al término de la asignatura, el estudiante examinará cómo los ciberdelincuentes actúan para poder combatir, mitigar y paliar cualquier tipo de amenaza en los sistemas; es así como, gracias al conocimiento de las técnicas y vectores que utilizan estos ciberdelincuentes, podrá evaluar la información suficiente para el tratamiento ético.

En ese sentido, conocerá los pasos y mecanismos necesarios para completar un ataque cibernético y cómo mitigarlos, para ello, se incluirán todos los pasos de un examen de penetración (estándares, metodologías, herramientas y buenas prácticas) para seguir las pautas y metodologías actuales que reforzará en la obtención de información.

Asimismo, analizará las diferentes técnicas, métodos y metodologías de análisis y funcionamiento de código malicioso como troyanos, virus, rootkits, entre otros, con el propósito de evaluar el daño causado, diseñar medidas técnicas para su defensa y valorar las intenciones y capacidades de un atacante e implementar un laboratorio de análisis de programas malignos seguros, de forma que se eviten accidentes de evasiones de estos.

Código 204 – MC
Mecanismos Criptográficos, de Autenticación y Control de Acceso

Al término de la asignatura, el estudiante destacará las bases y herramientas de trabajo necesarias para entender la problemática de la seguridad en redes móviles y redes virtuales, profundizando en los aspectos tecnológicos más relevantes y específicos de estas tecnologías, con el objetivo de desarrollar las estrategias necesarias para crear un entorno de trabajo seguro.

Además, comprenderán la importancia de la tecnología de la información digital, evaluando las bases de los medios de identificación electrónica, con la finalidad de proyectar e incorporar las utilidades de la identificación corporal.

Código 205 – MC
Metodología de la Investigación II

La asignatura es de carácter tiene como propósito desarrollar en los maestrantes competencias cognitivas que le permitan conocer y dominar el proceso de la investigación científica en su enfoque cualitativo, cuantitativo y mixto. Se revisa el método para que los alumnos puedan formular un problema de investigación, construir las hipótesis y objetivos, así como plantear la justificación que permita validar el desarrollo de la labor investigativa.

1.2. Sumilla de las asignaturas de complementación académica

1.2.1. Sumilla de Metodologías Ágiles

Código 301
Design Thinking

La asignatura desarrolla conceptos básicos de design thinking, el pensamiento de diseño y los ámbitos a los que se aplica, requisitos previos que se deben cumplir, los procesos para la implementación de esta metodología, etapas del pensamiento de diseño.

Código 302
Estrategia Lean

El participante se familiariza con las metodologías ágiles, conoce conceptos y herramientas del pensamiento ágil que permitan el éxito en la mejora de procesos o la creación de negocios con una mayor velocidad y eficiencia, considerando el ahorro de tiempo y costos, y alcanzando la satisfacción del cliente.

Código 303
Scrum

El participante desarrolla este sistema de trabajo que permite realizar el doble trabajo en la mitad de tiempo. Comprende los aspectos a tener en consideración para la reducción del papeleo, la burocracia y la jerarquización en las empresas y los proyectos, y apuesta por las prácticas colaborativas para generar involucramiento en las actividades que se realizan, trabajo rápido y el alcance de los objetivos trazados.

1.2.2. Sumilla de la Dirección de Proyectos

Código 401
Gestión de las adquisiciones y los interesados

Cuando tratamos la gestión de las adquisiciones de un Proyecto el departamento de compras adquiere una relevancia mayor que cualquier otro departamento de una empresa. Los Project Manager no deben conocer bien el área de las adquisiciones y saber los diferentes tipos de contratos más utilizados y quienes son los interesados y como impactan estas adquisiciones en sus intereses.

Código 402
Integración y alcance de proyectos

En el contexto de la dirección de proyectos, la integración incluye características de unificación, consolidación, articulación, así como las acciones integradoras que son cruciales para la terminación del proyecto, la gestión exitosa de las expectativas de los interesados y el cumplimiento de los requisitos. Por otro lado, el término alcance está referido al trabajo que debe realizarse para entregar los productos, servicios o resultados con las características y funciones especificadas.

Código 403
Gestión de las comunicaciones y del riesgo

En la gestión de la comunicación del proyecto, los directores de Proyecto deben asegurar que se entrega el mensaje adecuado, a la audiencia del Proyecto adecuada, y en el momento adecuado. Siendo fundamental para dirigir el Proyecto hacia el éxito y minimizar los riesgos.

1.3. Perfil del Ingresante

Grado académico de bachiller y/o título profesional en áreas relacionadas con Sistemas de Computación, Ingeniería en Sistemas Computacionales o Ingeniería en Redes, Ingenieros en Informática, Telecomunicaciones o Telemática. Ingenierías relacionadas con las TICs.

La Comisión de Admisión podrá considerar la experiencia profesional para el proceso de admisión.

1.3.1. Conocimientos sobre

- Interés por la seguridad informática.

1.3.2. Habilidades

- Capacidad de abstracción, análisis, síntesis y razonamiento lógico.
- Poseer capacidad de percepción y atención.

1.3.3. Actitudes

- Actitud abierta y capacidad de análisis.
- Capacidad de comunicación, relación social y trabajo en equipo.
- Autodisciplina.
- Dominio medio de inglés tanto escrito como leído.
- Disponer de sentido práctico de la organización.

1.4. Objetivo general del programa

Los egresados de la Maestría en Ciberseguridad serán capaces de analizar los riesgos de los sistemas de información relacionados con la seguridad en todo tipo de sistemas y de aplicar los procesos de gestión y mejora de la seguridad en las organizaciones, a través de conocer los principales estándares y buenas prácticas de auditoría de la seguridad, valorar los diferentes algoritmos y técnicas criptográficas y los mecanismos de protección asociados a ellas. Para ello, comprenderá los elementos de gestión de seguridad de la información, seguridad en redes y la comercialización de servicios de seguridad informática, las plataformas hardware especializadas para la seguridad informática y el concepto de vulnerabilidad, así como su tipología; complementariamente, conocerá las principales técnicas de protección frente a ataques y amenazas en los sistemas operativos, las redes, el software de aplicación, los sistemas web y las bases de datos, con la finalidad de ser capaz de proponer y diseñar normas, procedimientos métodos y técnicas confiables e innovadoras, así como aplicar correctamente las principales técnicas de análisis forense en materia de ciberseguridad.

De igual forma, podrá argumentar, discutir juicios y evaluar aspectos relacionados a la vulnerabilidad de redes, tecnologías de identificación digital, diseño y desarrollo de los programas informáticos seguros, asumiendo valores éticos en su desarrollo profesional.

1.5. Objetivos específicos de formación

- Formar profesionales expertos en ciberseguridad.
- Formar profesionales con los conocimientos y competencias más actualizadas y relevantes para analizar, diseñar y gestionar la ciberseguridad.
- Preparar profesionales capaces de desarrollarse en carreras profesionales en el ámbito de la ciberseguridad, desde el diseño de soluciones técnicas hasta la gestión de procesos y auditorías o la consultoría en riesgos legales.

1.6. Perfil del Egresado

El perfil que deben lograr los egresados es el siguiente:

1.6.1. Conocimientos

- La contratación de servicios informáticos; haciendo uso de los elementos jurídicos que protegen el desarrollo de los programas informáticos.
- Las tecnologías de identificación digital, para contar con sistemas actualizados de la información.
- Los sistemas y las metodologías de gestión de riesgos de los programas informáticos y los sistemas de gestión de riesgos, para implementar nuevas metodologías.
- Las tecnologías de las redes en entorno móviles y el desarrollo de sistemas de seguridad en entornos móviles.

- Sistemas de información y los tipos y niveles de auditoría, para desarrollar nuevas propuestas metodológicas.
- Las arquitecturas de las bases de datos masivos. Para determinar la importancia dentro de la seguridad informática.
- Las aplicaciones de seguridad informática en línea, para estructuras nuevos contenidos referentes a la seguridad.
- Revisar estándares, protocolos y métodos para fomentar el aspecto normativo.
- Búsqueda de mecanismos de seguridad para sistemas informáticos, para contar con las mejores opciones dentro de la seguridad informática.
- Fraudes dentro de la red y todo tipo de delincuencia informática.
- Los principales atacantes de los sistemas operativos para saber cómo combatirlos.
- Seguridad en base de datos masivos para su aplicación.
- Los documentos nacionales de identificación para contar con los fundamentos teóricos del sistema de base datos.
- Los distintos medios de identificación electrónica para programar plataformas de identificación digital.
- El diseño de seguridad de programas informáticos para mejorar el desarrollo en las técnicas de codificación segura.
- El funcionamiento, características y nivel de riesgo de los servicios de las empresas y establecer mecanismos de protección.
- Las variables necesarias para poder implementar un SGSI.
- Los distintos mecanismos cryptographic para seleccionar el óptimo en cada ámbito de aplicación.
- Las políticas de seguridad de la infraestructura de la red de la entidad.
- La normativa de centros de respuesta a incidentes de seguridad, infraestructuras críticas y principales conceptos de auditoría de sistemas.

1.6.2. Habilidades

- Analizar las vulnerabilidades, manejar los protocolos de seguridad, los mecanismos de defensa de redes.
- Utilizar y manejar los ficheros y buscar evidencias dado el uso de las diferentes herramientas para el análisis de evidencias.
- Emplear los procesos para detectar vulnerabilidades, clasificar y caracterizar los tipos de vulnerabilidades.
- Analizar los problemas de seguridad en las aplicaciones y en la prestación de los servicios en la red informática mundial.
- Conocer, comprender y utilizar la seguridad de los diferentes sistemas operativos y clasificar los tipos de atacantes a la misma.
- Caracterizar los medios de identificación electrónica, proyectar e incorporar las utilidades de la identificación corporal.
- Aplicar el criptoanálisis a sistemas de redes e informáticos y prevenir los ataques criptográficos.
- Manejar las características avanzadas de seguridad integrada a los sistemas operativos libres, además monitorizar y administrar los permisos de usuarios en Linux o Android.
- Aplicar las técnicas de codificación segura, prevenir y probar los programas informáticos para determinar su grado de seguridad.
- Aplicar los lineamientos de la estructura de investigación, argumentar cuales son los puntos medulares de la su implementación o innovación.
- Identificar y eliminar vulnerabilidades en el fraude o robo de la información.
- Manejar los programas, procesos y políticas de seguridad de la información.
- Diseñar instrumentos para la protección de la infraestructura computacional.
- Proteger la integridad de las bases de datos para asegurar la confidencialidad de la información sensible contenida.
- Implantar procesos de análisis forense de cualquier sistema informático.
- Diseñar, implantar e institucionalizar un proceso de análisis y gestión de riesgos de los sistemas de información en cualquier organización.
- Identificar, analizar y definir los riesgos de los servicios de las empresas para poder gestionarlos con criterio y de manera efectiva, en función de sus perfiles de seguridad.

- Discernir sobre los distintos entornos de seguridad existentes, tanto en local como en la nube, para poder seleccionar el óptimo siguiendo un razonamiento profesional y completo.
- Analizar el funcionamiento de herramientas de seguridad y su uso conjugado.
- Identificar y proceder contra aquellas conductas tipificadas como delito informático en el marco jurídico actual.
- Diseñar un plan de seguridad adaptado a las necesidades del entorno y su perfil de riesgos.
- Administrar las herramientas de seguridad para mejorar el SGSI impulsando la adecuada implantación en su infraestructura.
- Diseñar las correctas políticas para analizar y reproducir los hechos ante un incidente de seguridad informática.
- Asegurar la confidencialidad de los informes realizados para evitar comprometer los datos privados de la entidad.
- Analizar la infraestructura de red para poder determinar el nivel de riesgo de las soluciones técnicas y administrativas implantadas, tanto en entorno local como en la nube.
- Diseñar las políticas de recuperación de datos más adecuadas para disminuir el impacto ante incidentes.
- Manejar correctamente sistemas operativos, redes y lenguajes de programación desde el punto de vista de la seguridad informática y de las comunicaciones.
- Analizar y detectar amenazas de seguridad y desarrollar técnicas para su prevención.

1.6.3. Actitudes

- Adquirir una ética profesional para un asesoramiento y una toma de decisiones justa.
- Asesorar sobre las distintas medidas de seguridad aplicables a los sistemas informáticos para disminuir el impacto de sus posibles fallos.
- Tomar decisiones proactivas y reactivas frente los posibles fallos de seguridad, investigando las causas que las originan.
- Concientizarse y concientizar sobre la gravedad de los delitos informáticos.
- Participación en trabajo grupal y colaborativo en beneficio de las instituciones donde labora.
- Concientizar a los usuarios informáticos del debido uso y aplicación de los sistemas.
- Desarrollar e integrar un asesoramiento en seguridad que fomente una actitud proactiva y responsable hacia la seguridad informática en todos los niveles.
- Adquirir una visión general e integrada del asesoramiento en seguridad que permita la colaboración con otros departamentos de la entidad.
- Acciones éticas propias de un jefe de seguridad informática logrando la comprensión racional de principios éticos y su correcto empleo en su ejercicio profesional.
- Compromiso y participación con el desarrollo y enriquecimiento de los temas relacionados con la seguridad informática.
- Crítico en sus actividades laborales, con el fin de superarse y mejorar su desempeño profesional.
- Objetividad para el diseño y desarrollo de programas informáticos.
- Apertura al cambio en la implementación de la tecnología y en las nuevas áreas de la seguridad informática.
- Honestidad y apego a las normas necesarias de su práctica profesional.

1.7. Perfil Docente:

Los docentes deben contar con el siguiente perfil:

- Poseer grado de maestro y/o doctor.
- Formación relacionada al programa.
- Experiencia docente y/o profesional en la materia a desarrollar.

1.8. Grado que se obtiene:

Al finalizar los estudios el estudiante podrá optar el grado de **Maestro en Ciberseguridad.**

Newman
Escuela de Posgrado