María Cano
Fundación Universitaria
Vigilada MinEducación

POSGRADOS María Cano

Medellín

Especialización EN CIBERSEGURIDAD

SNIES 110866 RC No.000917 del 31 de enero de 2022

Duración 2 semestres

Modalidad Presencial

Número de creditos 29 créditos

Título que otorga Especialista en Ciberseguridad

Presentación **general**

La Fundación Universitaria María Cano ofrece el programa de posgrado en Especialización en Ciberseguridad bajo modalidad presencial, en consonancia con la Ley 30 de 1992. La Ciberseguridad es un elemento estratégico organizacional donde se pretende que uno de los objetivos del área encargada de las tecnologías de la información y las comunicaciones sea la de asumir la responsabilidad de salvaguardar la información a través de mecanismos y herramientas tecnológicas y del poder otorgado por la legislación nacional ajustada a los postulados internacionales.

Sin duda, en todo el proceso de expansión y evolución de las industrias que se lleva en la actualidad, la información toma un valor fundamental y estratégico, convirtiéndose en pieza vital para el desarrollo de éstas, esto obliga a que las organizaciones hagan una labor eficiente en el proceso de gestión de la información y las tecnologías asociadas a esta de una manera integral y eficaz.

En un mundo que se ha vuelto dependiente de la información y de la tecnología, internet se convierte en un entorno que permite el envío y recepción de información desde cualquier parte del mundo, sin tener restricciones de tiempo ni espacio, con velocidades altas en la transferencia de datos, pero todo esto se ve enfrentado a una serie de riesgos que pueden llegar a sus vulnerabilidades, aumentando de manera significativa el número de amenazas latentes. Las organizaciones al entender todos los peligros presentes en la Web han comenzado a realizar grandes inversiones para buscar tener un entorno seguro para la información y para las tecnologías asociadas a ella, para mantener así protegido lo que hoy se ha convertido en uno de los activos más importantes en las organizaciones como lo es la información, máxime ahora que las empresas están sufriendo grandes transformaciones hacia las industrias 4.0, donde la conectividad, el uso de tecnologías y la transferencia de información digital se hacen fundamentales para el logro de los objetivos.

Teniendo en cuenta lo anterior, la Especialización en Ciberseguridad tiene como objetivo darle un valor agregado a la organización de tal forma que ésta cree un vínculo lo suficientemente fuerte entre las áreas de sistemas y seguridad que lleven a tomar decisiones acertadas en la escogencia del personal y las herramientas tecnológicas adecuadas para garantizar la integridad, la disponibilidad y la confidencialidad de la información de la empresa.

Perfil **Profesional**

El Especialista en Ciberseguridad será una persona responsable, creativa, con iniciativa y asertividad. Será Proactivo en la prevención y neutralización de riesgos que puedan afectar la seguridad de la información, así como aplicar métodos para la recuperación de la información ante incidentes de seguridad que se puedan presentar en la organización, de igual manera, será un líder en la implementación, desarrollo y aplicación de técnicas, métodos y herramientas orientadas a brindar protección a la información empresarial.

Perfil **ocupacional**

A continuación, se mencionan los campos de desempeño del Especialista en Ciberseguridad:

- Diseñar y ejecutar estrategias para enfrentar ciberataques.
- Proteger los activos de información de las compañías.
- Implementar la ciber resiliencia en los procesos críticos organizacionales para garantizar la continuidad del negocio.
- De igual forma, para resolver los problemas de seguridad de la información el Especialista en Ciberseguridad debe, desde la función de Identificación, desarrollar un entendimiento organizacional para administrar el riesgo de ciberseguridad para sistemas, personas, activos, datos y capacidades. Esta primera función la obtendrá con la asignatura Gestión de Riesgos, que le permitirá conocer y aplicar los métodos más usados para la identificación y tratamiento de riesgos de seguridad presentes en el ciberespacio.
- Desde la función de Protección admite la capacidad de limitar o contener el impacto de un posible evento de ciberseguridad; dentro de esta función se incluyen: administración de identidad y control de acceso; concientización y formación; seguridad de datos; procesos y procedimientos de protección de la

información; mantenimiento; y tecnología de protección. La asignatura Inteligencia de Amenazas busca que el especialista tenga las competencias para controlar y predecir incidentes mediante una serie de investigaciones y análisis de logs posibilitando que entiendan el proceso de Ciberinteligencia y ayudando a proteger la información e infraestructura critica de las organizaciones. Una segunda asignatura: Controles de Protección en Ciberseguridad permitirá que el estudiante aprenda a implementar controles que ayudaran a mantener segura la información y la infraestructura dando respuesta al proceso de protección del Framework de ciberseguridad.

- En cuanto a la tercera función de Detectar, se pretende desarrollar e implementar actividades apropiadas para detectar la ocurrencia de un evento de ciberseguridad, mediante los contenidos de la asignatura de Detección de Intrusiones, donde el estudiante aprenderá y aplicará las diferentes técnicas y herramientas que le permitan la detección de intrusiones en el ciberespacio, lo que le dará herramientas para poder mitigar y controlar cualquier ciberataque que se presenta y ponga en riesgo la infraestructura e información de las organizaciones.

- Por su parte, la función de Responder pretende desarrollar e implementar actividades apropiadas para tomar medidas con respecto a un incidente de ciberseguridad detectado, esta función incluye: planificación de respuesta, comunicaciones, análisis, mitigación, y mejoras. Con la asignatura Gestión de Incidentes y Ciberdefensa se busca que el estudiante aprenda a dar respuesta a cada incidente y ciberataque que se presente en la infraestructura critica de la organización de tal manera que se logre mitigar su impacto y se dé un proceso más ágil de recuperación del negocio y lo logrará adquiriendo las competencias que le permitirán realizar una evaluación basada en normas, estándares y mejores prácticas, al igual que la aplicación de una serie de procedimientos y políticas.

- Finalmente, la función de Recuperar exige desarrollar e implementar actividades apropiadas para mantener los planes de ciber resiliencia y restaurar cualquier capacidad o servicio que se haya deteriorado debido a un incidente de ciberseguridad. Con la asignatura Continuidad de Negocio que busca que el estudiante adquiera las competencias que le permitan prevenir, protegerse, y reaccionar ante los diferentes incidentes de seguridad que puedan llegar a afectar e impactar de forma negativa a las organizaciones. El propósito de esta asignatura es brindar a los estudiantes el conocimiento necesario

que permita se establezcan los planes de recuperación garantizando la continuidad del negocio y

Plan de **estudios**

Semestre 1 *Asignatura*	**Créditos**	
Ciberseguridad	3	N/A
Gestión de riesgos	3	N/A
Inteligencia de amenazas	3	N/A
Detección de intruciones	3	N/A
Seminario de investigación I	1	N/A

Total créditos 13

Semestre 2 *Asignatura*		
Aspectos legales de ciberseguridad	3	N/A
Controles de protección en ciberseguridad	3	N/A
Gestión de incidentes y ciberdefensa	3	N/A
Continuidad de negocio	3	N/A
Electiva	2	N/A
Seminario de investigación II	2	Seminario de investigación I

Total créditos 16

Total créditos 29

Más información

interesados@fumc.edu.co

304 598 2262 - **www.fumc.edu.co**

Para ingresar a cualquiera de los programas de postgrado que ofrece la institución el aspirante debe realizar el siguiente procedimiento según su condición de ingreso:

1- Diligenciar el formulario de inscripción en línea y enviar a la oficina de admisiones, registro y control académico los siguientes documentos en formato PDF:

a. Fotocopia autenticada del acta de grado del título de pregrado.

b. Certificado de experiencia laboral (no es indispensable).

c. Una fotocopia ampliada legible del documento de identidad.

d. Una foto tamaño 3X4, fondo azul claro.

e. Imprimir formato para pago de la inscripción por valor de $202.089, al finalizar la inscripción en línea.

f. Adjuntar formato de: Autorización para verificación de información académica (Visualizar y descargar aquí).

g. No se reciben documentos de manera física a menos que durante el proceso de admisión se requieran.

h. Presentar entrevista virtual.

i. Consultar listado de admitidos publicado en el portal institucional, oficina de admisiones.

*La Fundación se reserva el derecho de admisión y de asignar los horarios de estudio