Código de la Asignatura: IO11E3

Nombre del programa académico	Maestría en Investigación Operativa y Ciencia de Datos
Nombre completo de la asignatura	Ciberseguridad y Privacidad de los Datos
Área académica o categoría	Estadística Enfocada a la Ciencia de Datos
Semestre y año de actualización	Primer semestre de 2025
Tipo de asignatura	[ ] Obligatoria [x] Electiva
Número de créditos ECTS	5.22 ECTS
Intensidad horaria	10 horas Semanales – 40 Mensuales
Director o contacto del programa	Eliana Mirledy Toro Ocampo
Coordinador o contacto de la asignatura	Luis Fernando Galindres Guancha - lugal@utp.edu.co Google Scholar Luis Fernando Galindres

Descripción y Contenidos

1. Breve descripción

La asignatura se enfoca en proporcionar a los estudiantes las herramientas y técnicas necesarias para abordar problemas de toma de decisiones que involucran múltiples criterios o dimensiones, especialmente en entornos caracterizados por la incertidumbre y la subjetividad. A lo largo del curso, los alumnos aprenderán a estructurar y modelar problemas complejos, aplicar métodos fundamentales de jerarquización (ranking) y selección, como el Proceso Analítico Jerárquico (AHP), y los métodos de superación. Se hará énfasis en técnicas basadas en lógica difusa para manejar la ausencia de determinismo en los datos del problema, así como la subjetividad presente en los juicios humanos. El objetivo es desarrollar habilidades analíticas y de modelado que permitan tomar decisiones informadas, justificables y equilibradas en entornos empresariales, financieros y de políticas públicas.

2. Objetivos del programa académico

OP5. Fomentar dimensiones humanas que permitan generar espacios participativos de diálogo y reflexión con un enfoque sostenible, que contribuyan a la formación de profesionales capaces de abordar desafíos de manera integral y responsable.

Objetivos de la asignatura

OA1. Comprender los principios fundamentales de ciberseguridad aplicados a la analítica de datos, incluyendo conceptos de privacidad, integridad y confidencialidad de los datos analíticos.OA2. Desarrollar habilidades para identificar y evaluar riesgos y amenazas cibernéticas específicas en el contexto de proyectos de analítica de datos. OA3. Implementar medidas y técnicas de seguridad para proteger los datos durante todo el ciclo de vida analítico, desde la recolección hasta la interpretación de resultados. OA4. Aplicar normativas y estándares de seguridad en el manejo y análisis de datos, asegurando el cumplimiento de regulaciones relevantes y mejores prácticas de la industria. OA5. Integrar estrategias de ciberseguridad en el desarrollo y despliegue de modelos y algoritmos de análisis de datos, garantizando la confiabilidad y protección de los insights generados.

3. Resultados de aprendizaje de la asignatura

RA1. Identificar y analizar riesgos y amenazas de seguridad en proyectos de analítica de datos, proponiendo soluciones efectivas para mitigarlos.RA2. Implementar medidas de seguridad adecuadas para proteger la privacidad y la integridad de los datos durante todo el proceso analítico.

RA3. Aplicar normativas y estándares de ciberseguridad en el manejo de datos analíticos, asegurando el cumplimiento con regulaciones y mejores prácticas de la industria. RA4. Diseñar y desplegar modelos y algoritmos de análisis de datos que integren estrategias de ciberseguridad, garantizando la protección y confiabilidad de los resultados obtenidos.

4. Contenido

T1. Introducción a la ciberseguridad para ciencia de datos (29 h: 8 h con docente y 21 h independientes): Fundamentos de ciberseguridad: privacidad, integridad y confidencialidad, amenazas y vulnerabilidades en proyectos de analítica de datos, importancia de la ciberseguridad en la ciencia de datos aplicada.

T2. Gestión de riesgos y evaluación de amenazas (29 h: 8 h con docente y 21 h independientes): Identificación y análisis de riesgos cibernéticos en proyectos de analítica, métodos de evaluación de amenazas y vulnerabilidades, planificación de medidas de mitigación de riesgos.

T3. Medidas de seguridad en el ciclo de vida analítico (29 h: 8 h con docente y 21 h independientes): Seguridad en la recolección y almacenamiento de datos, protección de datos durante el procesamiento y análisis, seguridad en la interpretación y comunicación de resultados.

T4. Cumplimiento normativo y estándares de seguridad (29 h: 8 h con docente y 21h independientes): Normativas y regulaciones de protección de datos aplicadas a la ciencia de datos, estándares de seguridad y mejores prácticas en la industria, implementación de políticas de seguridad y gestión de cumplimiento.

T5. Integración de ciberseguridad en modelos y algoritmos (28 h: 8 h con docente y 20h independientes): Diseño seguro de modelos y algoritmos de análisis de datos, implementación de medidas de seguridad en código y sistemas, evaluación de la robustez y confiabilidad de modelos seguros.

5. Requisitos

- Conocimientos básicos de manejo de bases de datos y ciencia de datos aplicada. Nociones generales de sistemas y redes.

6. Recursos

● Johnson, M. (2018). Ciberseguridad y ciencia de datos: Protección de datos en un mundo interconectado. Editorial TechPress. ● Smith, R., & Jones, P. (2020). Seguridad de datos para analítica avanzada: Estrategias y mejores prácticas. Editorial DataSafe. ● García, L., & Pérez, A. (2019). Ciberseguridad: Una guía práctica para profesionales de ciencia de datos. Editorial CyberTech. ● Brown, K. (2017). Principios de ciberseguridad para analistas de datos. Revista Internacional de Ciencia de Datos, 5(2), 134-150. ●White, S. (2016). Gestión de riesgos y ciberseguridad en proyectos de ciencia de datos. En T. Miller (Ed.), Handbook of Data Analytics (pp. 287-305). Springer.

7. Herramientas técnicas de soporte para la enseñanza

Clases Magistrales, Se disponen de videos explicativos sobre los contenidos del curso.

8. Trabajos en laboratorio y proyectos

Durante el semestre el profesor implementa tareas y talleres que fomentan el aprendizaje, y lo relacionan con la especialidad de cada estudiante. Talleres por unidad (T1 a T5: 5 talleres de 6 horas, 30 horas). Proyecto de evaluación de riesgos y cumplimiento normativo en un proyecto de analítica (20 horas).

9. Métodos de aprendizaje: Metodologías activas, talleres y ejercicios de modelación

10. Métodos de evaluación: Exámenes parciales: 40%, Examen final: 30%, Tareas y proyectos: 30%