National University of Engineering (UNI)
School of Cybersecurity
Syllabus 2024-II

1. COURSE

CY281. Societal Security (Mandatory)

2. GENERAL INFORMATION

2.1 Course	:	CY281. Societal Security
2.2 Semester	:	10^{th} Semester.
2.3 Credits	:	3
2.4 Horas	:	2 HT; 2 HP;
2.5 Duration of the period	:	16 weeks
2.6 Type of course	:	Mandatory
2.7 Learning modality	:	Face to face
2.8 Prerrequisites	:	CY271. Organizational Security. (9^{th} Sem)

3. PROFESSORS

Meetings after coordination with the professor

4. INTRODUCTION TO THE COURSE

This course examines the intersection of cybersecurity and society, analyzing the impact of cybercrime, legislation, ethics, public policy, and privacy on society. The ethical and legal responsibilities of cybersecurity professionals are explored, as well as the social implications of emerging technologies.

5. GOALS

- Understand the ethical and legal dimensions of cybersecurity in a societal context.
- Analyze the impact of cybercrime and cybersecurity policies on society.
- Evaluate the social implications of emerging technologies in the field of cybersecurity.

6. COMPETENCES

3) Communicate effectively in a variety of professional contexts.. (Usage)

4) Recognize professional responsabilities and make informed judgments in computing practice based on legal and ethical principles. (Assessment)

6) Apply security principles and practices to maintain operations in the presence of risks and threats. (Usage)

7. TOPICS

Unit 1: cibercrimen (12 hours)	
Competences Expected: 3,4,6	
Topics	**Learning Outcomes**
• Comportamiento cibercriminal – La identificación de activos es la catalogación de activos de información en una organización, como bases de datos o hardware, para ayudar en la determinación del riesgo en caso de que los activos se vean comprometidos o se pierdan. Las amenazas incluyen cualquier evento que aproveche una vulnerabilidad que tenga el potencial de causar pérdidas o daños a la organización. Las organizaciones utilizan cada vez más la inteligencia de amenazas (modelado de amenazas) para mantener la conciencia y la capacidad reactiva ante amenazas existentes y emergentes. • Terrorismo cibernético – Actividades en el ciberespacio orientadas a generar miedo e incertidumbre en la sociedad. • Investigaciones cibercriminales – Métodos para investigar ataques cibernéticos por parte de delincuentes, organizaciones cibercriminales, adversarios extranjeros y terroristas. • Economía del cibercrimen – Los riesgos del cibercrimen son demasiado bajos, mientras que las recompensas son demasiado altas – El uso de criptomonedas (irrastreables) para cometer delitos cibernéticos en línea y en la Dark Web (bitcoin).	• Analice los diversos motivos del comportamiento de delito cibernético [Usar] • Resuma las actividades terroristas en el ciberespacio orientadas a generar miedo y certeza en la sociedad [Usar] • Describir métodos para investigar crímenes tanto nacionales como internacionales [Usar] • Explique por qué es necesario preservar la cadena de evidencia digital para perseguir los delitos cibernéticos [Usar]
Readings : [**shepherd2019introduction**], [**brittain2016cybercrime**]	

Unit 2: cibercrimen (10 hours)	
Competences Expected: 3,4,6	
Topics	**Learning Outcomes**
• Comportamiento cibercriminal – La identificación de activos es la catalogación de activos de información en una organización, como bases de datos o hardware, para ayudar en la determinación del riesgo en caso de que los activos se vean comprometidos o se pierdan. Las amenazas incluyen cualquier evento que aproveche una vulnerabilidad que tenga el potencial de causar pérdidas o daños a la organización. Las organizaciones utilizan cada vez más la inteligencia de amenazas (modelado de amenazas) para mantener la conciencia y la capacidad reactiva ante amenazas existentes y emergentes. • Terrorismo cibernético – Actividades en el ciberespacio orientadas a generar miedo e incertidumbre en la sociedad. • Investigaciones cibercriminales – Métodos para investigar ataques cibernéticos por parte de delincuentes, organizaciones cibercriminales, adversarios extranjeros y terroristas. • Economía del cibercrimen – Los riesgos del cibercrimen son demasiado bajos, mientras que las recompensas son demasiado altas – El uso de criptomonedas (irrastreables) para cometer delitos cibernéticos en línea y en la Dark Web (bitcoin).	• Analice los diversos motivos del comportamiento de delito cibernético [Usar] • Resuma las actividades terroristas en el ciberespacio orientadas a generar miedo y certeza en la sociedad [Usar] • Describir métodos para investigar crímenes tanto nacionales como internacionales [Usar] • Explique por qué es necesario preservar la cadena de evidencia digital para perseguir los delitos cibernéticos [Usar]
Readings : [**Brenner2007**]	

Unit 3: Ley cibernetica (12 hours)	
Competences Expected: 3,4	
Topics	**Learning Outcomes**
• Fundamentos constitucionales del derecho cibernético – Poder Ejecutivo – Poder Legislativo – Primera Enmienda – Cuarta enmienda – Décima enmienda • Propiedad intelectual relacionada con la ciberseguridad – El alcance, el costo y el entorno legal relacionados con el robo cibernético de propiedad intelectual. – El contenido específico estará impulsado por el país de enfoque. En los EE. UU., cubra la Sección 1201 de la Ley de Derechos de Autor del Milenio Digital. – Antielusión: Ley de derechos de autor del milenio digital (DMCA 1201) • Leyes de privacidad – Leyes que rigen la privacidad en Internet – Leyes que rigen la privacidad de las redes sociales – Leyes de vigilancia electrónica, como la Ley de escuchas telefónicas, la Ley de comunicaciones almacenadas y la Ley de registro de bolígrafos. • ley de seguridad de datos – Sección 5 de la Comisión Federal de Comercio de EE. UU. – Leyes estatales de seguridad de datos – Leyes estatales de notificación de violaciones de datos – Ley de Responsabilidad y Portabilidad del Seguro Médico (HIPAA) – Ley Gramm Leach Bliley (GLBA) – Intercambio de información a través de US-CERT, Ley de Ciberseguridad de 2015 • Leyes de piratería informática – Leyes federales sobre delitos informáticos de EE. UU., como la Ley de abuso y fraude informático. La mayoría de los delitos de piratería informática se procesan en virtud de la Ley de Abuso y Fraude Informático de los EE. UU. – Se necesita un marco y cooperación internacionales para procesar a los piratas informáticos extranjeros. • evidencia digital	• Analice los diversos motivos del comportamiento de delito cibernético [Usar] • Resuma las actividades terroristas en el ciberespacio orientadas a generar miedo y certeza en la sociedad [Usar] • Describir métodos para investigar crímenes tanto nacionales como internacionales [Usar] • Explique por qué es necesario preservar la cadena de evidencia digital para perseguir los delitos cibernéticos [Usar] • Describir los fundamentos constitucionales del derecho cibernético [Usar] • Describir las leyes internacionales de seguridad de datos y piratería informática [Usar] • Interpretar las leyes de propiedad intelectual relacionadas con la seguridad [Usar] • Resumir las leyes que rigen la privacidad en línea [Usar]

Unit 4: Ética cibernética (10 hours)	
Competences Expected: 3,4	
Topics	**Learning Outcomes**
• Definiendo la ética – Compare y contraste las principales posturas éticas, incluida la ética de la virtud, la ética utilitaria y la ética deontológica. – Aplicar las tres posturas éticas diferentes al pensar en las consecuencias éticas de un problema o acción en particular. • Ética profesional y códigos de conducta. – Principales sociedades profesionales, como ACM, IEEE-CS, AIS y (ISC)2 – Responsabilidad profesional – Responsabilidad ética en relación con la vigilancia • Ética y equidad/diversidad – Describir las formas en que los algoritmos de toma de decisiones pueden sobrerrepresentar o subrepresentar a los grupos mayoritarios y minoritarios en la sociedad. – Analizar las formas en que los algoritmos pueden incluir implícitamente sesgos sociales, de género y de clase. • Ética y derecho – Comprender que es posible que las prácticas éticas y los códigos legales no siempre se alineen exactamente – Las prácticas éticas pueden considerarse universales, mientras que las leyes pueden ser específicas de una nación o región (por ejemplo, la Unión Europea). – Las leyes pueden evolucionar, pero los valores éticos pueden describirse como inmutables. • Autonomía/ética de los robots – Definir la toma de decisiones autónoma – Definir la inteligencia artificial y describir los dilemas éticos que presenta el uso o empleo de la inteligencia artificial (IA). – Describir los avances legislativos que han definido la personalidad y la personalidad digital. – Describir el conflicto creado por las nociones legales de responsabilidad y el uso de programas de toma de decisiones autónomos o no tripulados. • Ética y conflicto – Principios de Guerra Justa al ciberespacio en relación con el inicio de conflictos, comportamientos en conflicto, cese de conflicto/situación post-conflicto	• Distinguir entre ética de la virtud, ética utilitaria y ética deontológica [Usar] • Parafrasee la ética profesional y los códigos de conducta de sociedades profesionales destacadas, como ACM, IEEE-CS, AIS y (ISC)2 [Usar] • Describir formas en las que los algoritmos de toma de decisiones podrían sobrerrepresentar o subrepresentar a los grupos mayoritarios y minoritarios en la sociedad [Usar]

Unit 5: Política cibernética (8 hours)	
Competences Expected: 3,4	
Topics	**Learning Outcomes**
• Política cibernética internacional – Desafíos de la política cibernética internacional – Ley Internacional de Supervisión de la Política Cibernética de 2015 – Estrategia de política internacional del ciberespacio del Departamento de Estado • Política cibernética federal de EE. UU. – Ley Federal de Modernización de la Seguridad de la Información, una actualización de las políticas y directrices de ciberseguridad del Gobierno Federal – Relación con la infraestructura crítica de la nación – Gestionar el riesgo a nivel nacional • Impacto global – Efectos de la ciberseguridad en el sistema internacional en general y en la seguridad internacional en particular. – Cómo lo cibernético se ha convertido y seguirá convirtiéndose en un instrumento de poder, y cómo este poder podría cambiar el equilibrio de poder entre países más fuertes y más débiles. – Gobernanza global de la cibernética. Examinar también las posibilidades del desarrollo de comportamientos normativos relacionados con el uso de lo cibernético. – Efectos de la cibernética en la economía global. • Política de ciberseguridad y seguridad nacional – Cómo define un país su política, doctrina y responsabilidad de ejecución en materia de ciberseguridad, incluida la política, la arquitectura, las señales y las narrativas nacionales en materia de ciberseguridad, y la coerción y el blasón – Los mensajes de ciberseguridad de una nación; cómo señala sus intenciones de ganar la atención y la cooperación de otras naciones • Implicaciones económicas nacionales de la ciberseguridad – El costo de la ciberseguridad para una nación – Las pérdidas y ganancias de la ciberseguridad para una nación – La inversión para mantener a una nación protegida de ciberamenazas y ciberataques. • Nuevas adyacencias a la diplomacia – El “baile delicado” de la ciberdiplomacia – Aspectos de la ciberseguridad que se han con-	• Describir las principales posiciones de política pública internacional y el impacto que tienen en organizaciones e individuos [Usar] • Resumir la política pública de ciberseguridad específica de cada país con respecto a la protección de información sensible y protección de infraestructura crítica [Usar] • Explicar el impacto global de la ciberseguridad en la cultura, incluidas áreas como la economía, las cuestiones sociales, las políticas y las leyes [Usar] • Distinguir entre ética de la virtud, ética utilitaria y ética deontológica [Usar] • Parafrasee la ética profesional y los códigos de conducta de sociedades profesionales destacadas, como ACM, IEEE-CS, AIS y (ISC)2 [Usar] • Describir formas en las que los algoritmos de toma de decisiones podrían sobrerrepresentar o subrepresentar a los grupos mayoritarios y minoritarios en la sociedad [Usar]

Unit 6: Privacidad (8 hours)	
Competences Expected: 3,4,6	
Topics	**Learning Outcomes**
• Definiendo privacidad – Aplicar definiciones operativas de privacidad – Identificar diferentes objetivos de privacidad, por ejemplo, confidencialidad de las comunicaciones y privacidad de los metadatos. – Identificar compensaciones en materia de privacidad: aumentar la privacidad puede tener riesgos (por ejemplo, el uso de Tor podría convertir a alguien en blanco de un mayor escrutinio gubernamental en algunas partes del mundo). • Derechos de privacidad – Describir las condiciones del consentimiento informado en relación con la recopilación y el intercambio de datos personales. – Reconocer los derechos nacionales de privacidad en la existencia de derechos de privacidad, – Demostrar familiaridad con el debate sobre el derecho humano universal a la privacidad. • Salvaguardar la privacidad – Enumere los pasos de ciberhigiene para salvaguardar la privacidad personal – Enumere las tecnologías que mejoran la privacidad y su uso y las propiedades que proporcionan y no proporcionan (es decir, Tor, cifrado). – Describir las condiciones para el uso ético y legal de tecnologías que mejoran la privacidad. – Describir los pasos para llevar a cabo una evaluación del impacto en la privacidad. – Describir el papel del administrador de datos. – Describir la legislación relacionada con las prácticas de localización de datos. – Demostrar una comprensión de la diferencia entre los derechos de privacidad y la capacidad de mejorar la privacidad: operacionalizar la privacidad. – Discutir el impacto dinámico de los metadatos y big data en la privacidad • Normas y actitudes de privacidad. – Teoría y modelo del cálculo de privacidad. – Diferencias culturales en la existencia de normas y límites de privacidad. • Violaciones de privacidad – Este tema cubre el papel de las corporaciones en la protección de datos y abordar circunstancias en las que la privacidad de los datos se ve comprometida. • Privacidad en las sociedades	• Describir el concepto de privacidad, incluida la definición social de lo que constituye información personalmente privada y las compensaciones entre privacidad y seguridad individual [Usar] • Resuma el equilibrio entre los derechos a la privacidad del individuo y las necesidades de la sociedad [Usar] • Describir las prácticas y tecnologías comunes utilizadas para salvaguardar la privacidad personal [Usar]

8. WORKPLAN

8.1 Methodology

Individual and team participation is encouraged to present their ideas, motivating them with additional points in the different stages of the course evaluation.

8.2 Theory Sessions

The theory sessions are held in master classes with activities including active learning and roleplay to allow students to internalize the concepts.

8.3 Practical Sessions

The practical sessions are held in class where a series of exercises and/or practical concepts are developed through problem solving, problem solving, specific exercises and/or in application contexts.

9. EVALUATION SYSTEM

********* EVALUATION MISSING ********

10. BASIC BIBLIOGRAPHY