Universidad Nacional de Ingeniería (UNI)
Escuela Profesional de
Ciberseguridad
Sílabo 2024-II

1. CURSO

CY281. Seguridad Social (Obligatorio)

2. INFORMACIÓN GENERAL

2.1 Curso	:	CY281. Seguridad Social
2.2 Semestre	:	10^{mo} Semestre.
2.3 Créditos	:	3
2.4 horas	:	2 HT; 2 HP;
2.5 Duración del periodo	:	16 semanas
2.6 Condición	:	Obligatorio
2.7 Modalidad de aprendizaje	:	Presencial
2.8 Prerrequisitos	:	CY271. Seguridad Organizacional. (9^{no} Sem)

3. PROFESORES

Atención previa coordinación con el profesor

4. INTRODUCCIÓN AL CURSO

Este curso examina la intersección entre la ciberseguridad y la sociedad, analizando el impacto del cibercrimen, la legislación, la ética, las políticas públicas y la privacidad en la sociedad. Se exploran las responsabilidades éticas y legales de los profesionales de la ciberseguridad, así como las implicaciones sociales de las tecnologías emergentes.

5. OBJETIVOS

- Comprender las dimensiones éticas y legales de la ciberseguridad en el contexto social.
- Analizar el impacto del cibercrimen y las políticas de ciberseguridad en la sociedad.
- Evaluar las implicaciones sociales de las tecnologías emergentes en el ámbito de la ciberseguridad.

6. RESULTADOS DEL ESTUDIANTE

3) ()

4) ()

6) Aplicar principios y prácticas de seguridad para mantener las operaciones en presencia de riesgos y amenazas.()

7. TEMAS

Unidad 1: cibercrimen (10 horas)	
Resultados esperados: 3,4,6	
Temas	**Objetivos de Aprendizaje**
• 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]
Lecturas : [**Brenner2007**]	

Unidad 2: Ley cibernetica (12 horas)	
Resultados esperados: 3,4	
Temas	**Objetivos de Aprendizaje**
• 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]

Unidad 3: Ética cibernética (10 horas)	
Resultados esperados: 3,4	
Temas	**Objetivos de Aprendizaje**
• 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]

Unidad 4: Política cibernética (8 horas)	
Resultados esperados: 3,4	
Temas	**Objetivos de Aprendizaje**
• 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]

Unidad 5: Privacidad (8 horas)	
Resultados esperados: 3,4,6	
Temas	**Objetivos de Aprendizaje**
• 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. PLAN DE TRABAJO

8.1 Metodología

Se fomenta la participación individual y en equipo para exponer sus ideas, motivándolos con puntos adicionales en las diferentes etapas de la evaluación del curso.

8.2 Sesiones Teóricas

Las sesiones de teoría se llevan a cabo en clases magistrales donde se realizarán actividades que propicien un aprendizaje activo, con dinámicas que permitan a los estudiantes interiorizar los conceptos.

8.3 Sesiones Prácticas

Las sesiones prácticas se llevan en clase donde se desarrollan una serie de ejercicios y/o conceptos prácticos mediante planteamiento de problemas, la resolución de problemas, ejercicios puntuales y/o en contextos aplicativos.

9. SISTEMA DE EVALUACIÓN

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

10. BIBLIOGRAFÍA BÁSICA