



## 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 <sup>mo</sup> 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 <sup>no</sup> 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) Comunicarse efectivamente en diversos contextos profesionales. (Usage)
- 4) Reconocer las responsabilidades profesionales y tomar decisiones informadas en la práctica de la computación basadas en principios legales y éticos. (Assessment)
- 6) Aplicar principios y prácticas de seguridad para mantener las operaciones en presencia de riesgos y amenazas. (Usage)

### 7. TEMAS

Unidad 1: cibercrimen (10 horas)	
Resultados esperados: 3,4,6	
Temas	Objetivos de Aprendizaje ( <i>Learning Outcomes</i> )
<ul style="list-style-type: none"> <li>• Comportamiento cibercriminal <ul style="list-style-type: none"> <li>– 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.</li> </ul> </li> <li>• Terrorismo cibernético <ul style="list-style-type: none"> <li>– Actividades en el ciberespacio orientadas a generar miedo e incertidumbre en la sociedad.</li> </ul> </li> <li>• Investigaciones cibercriminales <ul style="list-style-type: none"> <li>– Métodos para investigar ataques cibernéticos por parte de delincuentes, organizaciones cibercriminales, adversarios extranjeros y terroristas.</li> </ul> </li> <li>• Economía del cibercrimen <ul style="list-style-type: none"> <li>– Los riesgos del cibercrimen son demasiado bajos, mientras que las recompensas son demasiado altas</li> <li>– El uso de criptomonedas (irrastreables) para cometer delitos cibernéticos en línea y en la Dark Web (bitcoin).</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Analice los diversos motivos del comportamiento de delito cibernético [Usar]</li> <li>• Resuma las actividades terroristas en el ciberespacio orientadas a generar miedo y certeza en la sociedad [Usar]</li> <li>• Describir métodos para investigar crímenes tanto nacionales como internacionales [Usar]</li> <li>• Explique por qué es necesario preservar la cadena de evidencia digital para perseguir los delitos cibernéticos [Usar]</li> </ul>
Lecturas : [Brenner2007]	

Unidad 2: Ley cibernética (12 horas)	
Resultados esperados: 3,4	
Temas	Objetivos de Aprendizaje ( <i>Learning Outcomes</i> )
<ul style="list-style-type: none"> <li>● Fundamentos constitucionales del derecho cibernético <ul style="list-style-type: none"> <li>– Poder Ejecutivo</li> <li>– Poder Legislativo</li> <li>– Primera Enmienda</li> <li>– Cuarta enmienda</li> <li>– Décima enmienda</li> </ul> </li> <li>● Propiedad intelectual relacionada con la ciberseguridad <ul style="list-style-type: none"> <li>– El alcance, el costo y el entorno legal relacionados con el robo cibernético de propiedad intelectual.</li> <li>– 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.</li> <li>– Antielusión: Ley de derechos de autor del milenio digital (DMCA 1201)</li> </ul> </li> <li>● Leyes de privacidad <ul style="list-style-type: none"> <li>– Leyes que rigen la privacidad en Internet</li> <li>– Leyes que rigen la privacidad de las redes sociales</li> <li>– Leyes de vigilancia electrónica, como la Ley de escuchas telefónicas, la Ley de comunicaciones almacenadas y la Ley de registro de bolígrafos.</li> </ul> </li> <li>● ley de seguridad de datos <ul style="list-style-type: none"> <li>– Sección 5 de la Comisión Federal de Comercio de EE. UU.</li> <li>– Leyes estatales de seguridad de datos</li> <li>– Leyes estatales de notificación de violaciones de datos</li> <li>– Ley de Responsabilidad y Portabilidad del Seguro Médico (HIPAA)</li> <li>– Ley Gramm Leach Bliley (GLBA)</li> <li>– Intercambio de información a través de US-CERT, Ley de Ciberseguridad de 2015</li> </ul> </li> <li>● Leyes de piratería informática <ul style="list-style-type: none"> <li>– 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.</li> <li>– Se necesita un marco y cooperación internacionales para procesar a los piratas informáticos extranjeros.</li> </ul> </li> <li>● evidencia digital</li> </ul>	<ul style="list-style-type: none"> <li>● Analice los diversos motivos del comportamiento de delito cibernético [Usar]</li> <li>● Resuma las actividades terroristas en el ciberespacio orientadas a generar miedo y certeza en la sociedad [Usar]</li> <li>● Describir métodos para investigar crímenes tanto nacionales como internacionales [Usar]</li> <li>● Explique por qué es necesario preservar la cadena de evidencia digital para perseguir los delitos cibernéticos [Usar]</li> <li>● Describir los fundamentos constitucionales del derecho cibernético [Usar]</li> <li>● Describir las leyes internacionales de seguridad de datos y piratería informática [Usar]</li> <li>● Interpretar las leyes de propiedad intelectual relacionadas con la seguridad [Usar]</li> <li>● Resumir las leyes que rigen la privacidad en línea [Usar]</li> </ul>

Unidad 3: Ética cibernética (10 horas)	
Resultados esperados: 3,4	
Temas	Objetivos de Aprendizaje ( <i>Learning Outcomes</i> )
<ul style="list-style-type: none"> <li>● Definiendo la ética <ul style="list-style-type: none"> <li>– Compare y contraste las principales posturas éticas, incluida la ética de la virtud, la ética utilitaria y la ética deontológica.</li> <li>– Aplicar las tres posturas éticas diferentes al pensar en las consecuencias éticas de un problema o acción en particular.</li> </ul> </li> <li>● Ética profesional y códigos de conducta. <ul style="list-style-type: none"> <li>– Principales sociedades profesionales, como ACM, IEEE-CS, AIS y (ISC)<sup>2</sup></li> <li>– Responsabilidad profesional</li> <li>– Responsabilidad ética en relación con la vigilancia</li> </ul> </li> <li>● Ética y equidad/diversidad <ul style="list-style-type: none"> <li>– Describir las formas en que los algoritmos de toma de decisiones pueden sobrerrepresentar o subrepresentar a los grupos mayoritarios y minoritarios en la sociedad.</li> <li>– Analizar las formas en que los algoritmos pueden incluir implícitamente sesgos sociales, de género y de clase.</li> </ul> </li> <li>● Ética y derecho <ul style="list-style-type: none"> <li>– Comprender que es posible que las prácticas éticas y los códigos legales no siempre se alineen exactamente</li> <li>– Las prácticas éticas pueden considerarse universales, mientras que las leyes pueden ser específicas de una nación o región (por ejemplo, la Unión Europea).</li> <li>– Las leyes pueden evolucionar, pero los valores éticos pueden describirse como inmutables.</li> </ul> </li> <li>● Autonomía/ética de los robots <ul style="list-style-type: none"> <li>– Definir la toma de decisiones autónoma</li> <li>– Definir la inteligencia artificial y describir los dilemas éticos que presenta el uso o empleo de la inteligencia artificial (IA).</li> <li>– Describir los avances legislativos que han definido la personalidad y la personalidad digital.</li> <li>– Describir el conflicto creado por las nociones legales de responsabilidad y el uso de programas de toma de decisiones autónomos o no tripulados.</li> </ul> </li> <li>● Ética y conflicto <ul style="list-style-type: none"> <li>– Principios de Guerra Justa al ciberespacio en relación con el inicio de conflictos, comportamientos en conflicto, cese de conflicto/situación post-conflicto</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>● Distinguir entre ética de la virtud, ética utilitaria y ética deontológica [Usar]</li> <li>● Parafrasee la ética profesional y los códigos de conducta de sociedades profesionales destacadas, como ACM, IEEE-CS, AIS y (ISC)<sup>2</sup> [Usar]</li> <li>● 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]</li> </ul>

Unidad 4: Política cibernética (8 horas)	
Resultados esperados: 3,4	
Temas	Objetivos de Aprendizaje ( <i>Learning Outcomes</i> )
<ul style="list-style-type: none"> <li>● Política cibernética internacional <ul style="list-style-type: none"> <li>– Desafíos de la política cibernética internacional</li> <li>– Ley Internacional de Supervisión de la Política Cibernética de 2015</li> <li>– Estrategia de política internacional del ciberespacio del Departamento de Estado</li> </ul> </li> <li>● Política cibernética federal de EE. UU. <ul style="list-style-type: none"> <li>– Ley Federal de Modernización de la Seguridad de la Información, una actualización de las políticas y directrices de ciberseguridad del Gobierno Federal</li> <li>– Relación con la infraestructura crítica de la nación</li> <li>– Gestionar el riesgo a nivel nacional</li> </ul> </li> <li>● Impacto global <ul style="list-style-type: none"> <li>– Efectos de la ciberseguridad en el sistema internacional en general y en la seguridad internacional en particular.</li> <li>– 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.</li> <li>– Gobernanza global de la cibernética. Examinar también las posibilidades del desarrollo de comportamientos normativos relacionados con el uso de lo cibernético.</li> <li>– Efectos de la cibernética en la economía global.</li> </ul> </li> <li>● Política de ciberseguridad y seguridad nacional <ul style="list-style-type: none"> <li>– 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</li> <li>– Los mensajes de ciberseguridad de una nación; cómo señala sus intenciones de ganar la atención y la cooperación de otras naciones</li> </ul> </li> <li>● Implicaciones económicas nacionales de la ciberseguridad <ul style="list-style-type: none"> <li>– El costo de la ciberseguridad para una nación</li> <li>– Las pérdidas y ganancias de la ciberseguridad para una nación</li> <li>– La inversión para mantener a una nación protegida de ciberamenazas y ciberataques.</li> </ul> </li> <li>● Nuevas adyacencias a la diplomacia <ul style="list-style-type: none"> <li>– El “baile delicado” de la ciberdiplomacia</li> <li>– Aspectos de la ciberseguridad que se han con-</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>● Describir las principales posiciones de política pública internacional y el impacto que tienen en organizaciones e individuos [Usar]</li> <li>● Resumir la política pública de ciberseguridad específica de cada país con respecto a la protección de información sensible y protección de infraestructura crítica [Usar]</li> <li>● Explicar el impacto global de la ciberseguridad en la cultura, incluidas áreas como la economía, las cuestiones sociales, las políticas y las leyes [Usar]</li> <li>● Distinguir entre ética de la virtud, ética utilitaria y ética deontológica [Usar]</li> <li>● Parafrasee la ética profesional y los códigos de conducta de sociedades profesionales destacadas, como ACM, IEEE-CS, AIS y (ISC)<sup>2</sup> [Usar]</li> <li>● 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]</li> </ul>

Unidad 5: Privacidad (8 horas)	
Resultados esperados: 3,4,6	
Temas	Objetivos de Aprendizaje ( <i>Learning Outcomes</i> )
<ul style="list-style-type: none"> <li>● Definiendo privacidad <ul style="list-style-type: none"> <li>– Aplicar definiciones operativas de privacidad</li> <li>– Identificar diferentes objetivos de privacidad, por ejemplo, confidencialidad de las comunicaciones y privacidad de los metadatos.</li> <li>– 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).</li> </ul> </li> <li>● Derechos de privacidad <ul style="list-style-type: none"> <li>– Describir las condiciones del consentimiento informado en relación con la recopilación y el intercambio de datos personales.</li> <li>– Reconocer los derechos nacionales de privacidad en la existencia de derechos de privacidad,</li> <li>– Demostrar familiaridad con el debate sobre el derecho humano universal a la privacidad.</li> </ul> </li> <li>● Salvaguardar la privacidad <ul style="list-style-type: none"> <li>– Enumere los pasos de ciberhigiene para salvaguardar la privacidad personal</li> <li>– Enumere las tecnologías que mejoran la privacidad y su uso y las propiedades que proporcionan y no proporcionan (es decir, Tor, cifrado).</li> <li>– Describir las condiciones para el uso ético y legal de tecnologías que mejoran la privacidad.</li> <li>– Describir los pasos para llevar a cabo una evaluación del impacto en la privacidad.</li> <li>– Describir el papel del administrador de datos.</li> <li>– Describir la legislación relacionada con las prácticas de localización de datos.</li> <li>– Demostrar una comprensión de la diferencia entre los derechos de privacidad y la capacidad de mejorar la privacidad: operacionalizar la privacidad.</li> <li>– Discutir el impacto dinámico de los metadatos y big data en la privacidad</li> </ul> </li> <li>● Normas y actitudes de privacidad. <ul style="list-style-type: none"> <li>– Teoría y modelo del cálculo de privacidad.</li> <li>– Diferencias culturales en la existencia de normas y límites de privacidad.</li> </ul> </li> <li>● Violaciones de privacidad <ul style="list-style-type: none"> <li>– 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.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>● 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]</li> <li>● Resuma el equilibrio entre los derechos a la privacidad del individuo y las necesidades de la sociedad [Usar]</li> <li>● Describir las prácticas y tecnologías comunes utilizadas para salvaguardar la privacidad personal [Usar]</li> </ul>

## **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**