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

1. COURSE

CY271. Organizational Security (Mandatory)

2. GENERAL INFORMATION

2.1 Course	:	CY271. Organizational Security
2.2 Semester	:	9^{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	:	CY261. Human Security. (8^{th} Sem)

3. PROFESSORS

Meetings after coordination with the professor

4. INTRODUCTION TO THE COURSE

This course focuses on information and system security from an organizational perspective. It covers risk management, security governance and policies, cybersecurity planning, business continuity, disaster recovery, systems administration, and personnel security, preparing students to implement comprehensive security programs in organizations.

5. GOALS

- Understand the principles and practices of risk management and security governance in organizations.
- Plan and implement cybersecurity programs that address organizational needs.
- Manage business continuity, disaster recovery, and personnel security.

6. COMPETENCES

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

5) Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline. (Usage)

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

7. TOPICS

Unit 1: Gestión de riesgos (10 hours)	
Competences Expected: 4,6	
Topics	**Learning Outcomes**
• Identificación de riesgos – 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. • Evaluación y análisis de riesgos. – El análisis de riesgos es el proceso organizacional para determinar y abordar posibles pérdidas accidentales o intencionales. – Diseñar e implementar procedimientos para minimizar el impacto de estas pérdidas. – También puede abarcar análisis de amenazas e inteligencia de amenazas. • Amenazas internas – Una persona privilegiada se define como cualquier persona con acceso autorizado a los recursos de una organización, incluido el personal, las instalaciones, la información, los equipos, las redes y los sistemas. – Una amenaza interna se define como el riesgo de que una persona interna utilice su acceso autorizado, consciente o inconscientemente, para dañar su organización. – Robo de información y tecnología patentadas; daños a las instalaciones, sistemas o equipos de la empresa; daño real o amenaza de daño a los empleados; u otras acciones que impidan a la empresa llevar a cabo sus prácticas comerciales normales. – Comportamientos motivo-medio-oportunidad: factores de motivación y disciplina, responsabilidad, conciencia y control de calidad. – El FBI ha desarrollado materiales que incluyen indicadores útiles para identificar posibles riesgos de amenazas internas. • Modelos y metodologías de medición y evaluación de riesgos – Enfoques tanto cuantitativos como cualitativos para la evaluación de riesgos, aplicación de modelos y métodos para diversos contextos comerciales (por ejemplo, HIPAA para instalaciones de atención médica).	• Describir la gestión de riesgos y su papel en la organización [Usar] • Describir técnicas de gestión de riesgos para identificar y priorizar factores de riesgo para activos de información y cómo se evalúa el riesgo [Usar] • Analice las opciones de estrategia utilizadas para tratar el riesgo y esté preparado para seleccionar entre ellas cuando se le proporcione información general [Usar] • Describir metodologías populares utilizadas en la industria para gestionar el riesgo [Usar]

Unit 2: Gobernanza y política de seguridad (12 hours)

Competences Expected: 4,5,6

Topics	Learning Outcomes
• Contexto organizacional – Las diferencias contextuales internas versus externas tienen un impacto importante en la cobertura de políticas, regulaciones y estatutos (o jurisdicción). – Se deben evaluar las cuestiones e inquietudes específicas de la ubicación o del país. – También se deben evaluar las normas y directrices aplicables para su cumplimiento por parte de la industria/sector. – La diferencia entre los gobiernos y las organizaciones privadas es un factor, al igual que la necesidad de incluir aspectos internacionales que incluyen, entre otros, restricciones a la importación y exportación. – Diferencia entre organizaciones en diversos segmentos industriales verticales de negocios, como energía versus agricultura. • Privacidad – Aborda las variaciones sociales y localizadas en la privacidad. – Se deben explorar las variaciones jurisdiccionales en las definiciones de privacidad. – También deben abordarse las relaciones entre individuos, organizaciones o los requisitos de privacidad gubernamentales. – El impacto de la configuración de privacidad en nuevas herramientas/software, identificando la necesidad de que las herramientas y técnicas se cubran en la mayoría de las áreas. • Leyes, ética y cumplimiento – Cómo las leyes y la tecnología se cruzan en el contexto de las estructuras judiciales presentes (internacionales, nacionales y locales) mientras las organizaciones protegen los sistemas de información de los ciberataques. – La instrucción ética también debería ser un elemento. – Deben abordarse los códigos de conducta profesionales y las normas éticas. – Ejemplos de leyes y estándares internacionales incluyen GDPR e ISO/IEC 27000 et al. Las leyes nacionales de importancia para las organizaciones estadounidenses incluyen HIPAA, Sarbanes-Oxley, GLBA, etc. – Los esfuerzos de cumplimiento deben incluir aquellos esfuerzos para cumplir con las leyes, regulaciones y estándares, e incluir requisitos de notificación de incumplimiento por parte de las autoridades gubernamentales estatales, nacionales e internacionales.	• Discuta la importancia, los beneficios y los resultados deseados de la gobernanza de la ciberseguridad y cómo se implementaría dicho programa [Usar] • Describir la política de seguridad de la información y su papel en un programa de seguridad de la información exitoso [Usar] • Describa los principales tipos de políticas de seguridad de la información y los principales componentes de cada una [Usar] • Explique qué es necesario para desarrollar, implementar y mantener una política efectiva y qué consecuencias puede enfrentar la organización si no lo hace [Usar] • Diferenciar entre derecho y ética [Usar] • Identificar leyes nacionales e internacionales importantes que se relacionen con la ciberseguridad. [Usar] • Explicar cómo las organizaciones logran el cumplimiento de las leyes y regulaciones nacionales e internacionales, y de los estándares industriales específicos [Usar] • Se debe dar mayor consideración a la privacidad en el contexto de las regulaciones de protección al consumidor y atención médica [Usar] • Las organizaciones con compromiso internacional deben considerar las variaciones en las leyes, regulaciones y estándares de privacidad en las jurisdicciones en las que operan [Usar] • Describa por qué los códigos de conducta éticos son importantes para los profesionales de la ciberseguridad y sus organizaciones [Usar]

Unit 3: Herramientas analiticas (8 hours)

Competences Expected: 4

Topics	Learning Outcomes
• Medidas de rendimiento (métricas) – Se deben explicar a los estudiantes los enfoques y técnicas para definir y evaluar la utilidad de las mediciones del desempeño. • Análisis de datos – Las diferencias entre software y herramientas de control de seguridad y análisis de seguridad; el tipo y clasificaciones de herramientas y técnicas analíticas (con ejemplos como OpenSOC); recopilar, filtrar, integrar y vincular diversos tipos de información de eventos de seguridad – Cómo funcionan las herramientas de análisis de seguridad – La relación entre el software y las herramientas analíticas y la ciencia forense. – Diferencias entre herramientas forenses y herramienta analítica – Análisis forense de red (para incluir análisis de paquetes, herramientas, Windows, Linux, UNIX, Mobile) – Diferencias entre ciberforense (redes sociales, por ejemplo) y forense de redes. • Inteligencia de seguridad – Se deben explorar herramientas y técnicas para incluir la recopilación y agregación de datos, la extracción de datos, el análisis de datos y el análisis estadístico. – Ejemplos de fuentes de inteligencia de seguridad incluyen SIEM para datos internos y servicios de inteligencia públicos y privados para datos externos. – La difusión incluye una comprensión del enfoque del Centro de análisis e intercambio de información, así como de organizaciones como InfraGard.	• Diferenciar entre derecho y ética [Usar] • Describa por qué los códigos de conducta éticos son importantes para los profesionales de la ciberseguridad y sus organizaciones [Usar] • Identificar leyes nacionales e internacionales importantes que se relacionen con la ciberseguridad. [Usar] • Explicar cómo las organizaciones logran el cumplimiento de las leyes y regulaciones nacionales e internacionales, y de los estándares industriales específicos [Usar]

Readings : [**NIST-SP800-137**]

Unit 4: Administración de Sistemas (8 hours)	
Competences Expected: 4,5,6	
Topics	**Learning Outcomes**
• Administración del sistema operativo – incluye, entre otros, gestión de cuentas, administraciones de discos, administración de procesos del sistema, automatización de tareas del sistema, monitoreo del rendimiento, optimización, administración de herramientas de seguridad y respaldo de discos y procesos. • Administración del sistema de base de datos. – pero no se limita a la instalación y configuración de servidores de bases de datos, creación y manipulación de esquemas, tablas, índices, vistas, restricciones, procedimientos almacenados, funciones, creación y administración de cuentas de usuario y herramientas para respaldo y recuperación de bases de datos. – La cobertura debe incluir las tecnologías de almacenamiento de datos de uso generalizado, así como las tecnologías emergentes de gestión de datos. • administración de red – incluye, entre otros, el modelo OSI, protección del tráfico de red y herramientas para la configuración de servicios. • administración de la nube – Este tema incluye, entre otros, la configuración e implementación de aplicaciones y usuarios en infraestructuras de nube. – analizando el desempeño – escalamiento de recursos – disponibilidad de plataformas en la nube – identificar problemas de seguridad y privacidad y mitigar riesgos. • Administración de sistemas ciberfísicos. – Incluye, entre otros, la arquitectura de los sistemas ciberfísicos. – Estándares de comunicación subyacentes (Zigbee). – software intermedio – Arquitectura orientada a Servicios – Herramientas que soportan el control en tiempo real y la aplicación de ejemplos del mundo real (red eléctrica, instalación nuclear, IoT, SCADA). • Endurecimiento del sistema – incluye, entre otros, la identificación de riesgos, amenazas y vulnerabilidades en sistemas de uso común (sistemas operativos, sistemas de bases de datos, redes)	• Diferenciar entre derecho y ética [Usar] • Describa por qué los códigos de conducta éticos son importantes para los profesionales de la ciberseguridad y sus organizaciones [Usar] • Identificar leyes nacionales e internacionales importantes que se relacionen con la ciberseguridad. [Usar] • Explicar cómo las organizaciones logran el cumplimiento de las leyes y regulaciones nacionales e internacionales, y de los estándares industriales específicos [Usar]

Unit 5: Planificación de ciberseguridad (10 hours)	
Competences Expected: 4,5	
Topics	**Learning Outcomes**
• Planificación estratégica – Cubre conceptos tales como determinar la posición actual de la organización. – realizar análisis de fortalezas, debilidades, oportunidades y amenazas (FODA); desarrollar una estrategia que cumpla con la misión, los valores y la visión de la organización; determinar objetivos a largo plazo; Seleccionar indicadores clave de rendimiento (KPI) para realizar un seguimiento del progreso. – asignar el presupuesto necesario – Implementar la estrategia en la organización y actualizarla y adaptarla anualmente. • Gestión Operativa y Táctica – Discusión sobre la protección de datos y la privacidad por defecto y diseño, y cubre conceptos, cuestiones y técnicas básicas para operaciones eficientes y efectivas. – Especial énfasis en la mejora de procesos y la gestión de la cadena de suministro. – Estrategias de operación – Estrategia táctica – Diseño de productos y servicios – Diseño y Análisis de procesos – Planificación de capacidad – Sistemas de producción lean – Gestion de materiales e inventarios – Gestión de calidad y seis sigma – Gestión de proyectos – Gestión de la cadena de suministro	• Explicar la planificación organizacional estratégica para la ciberseguridad y su relación con la planificación estratégica de TI y para toda la organización [Usar] • Identificar las partes interesadas clave de la organización y sus roles [Usar] • Describir los componentes principales de la planificación de la implementación del sistema de ciberseguridad [Usar]
Readings : [**Alberts2014**]	

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