



# Universidad Nacional de Ingeniería (UNI)

Escuela Profesional de

Ciberseguridad

Sílabo 2024-II

## 1. CURSO

CY271. Seguridad Organizacional (Obligatorio)

## 2. INFORMACIÓN GENERAL

2.1 Curso	:	CY271. Seguridad Organizacional
2.2 Semestre	:	9 <sup>no</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	:	CY261. Seguridad Humana. (8 <sup>vo</sup> Sem)

## 3. PROFESORES

Atención previa coordinación con el profesor

## 4. INTRODUCCIÓN AL CURSO

Este curso se centra en la seguridad de la información y los sistemas desde una perspectiva organizacional. Se abordan temas como gestión de riesgos, gobernanza y políticas de seguridad, planificación de la ciberseguridad, continuidad del negocio, recuperación ante desastres, administración de sistemas y seguridad de personal, preparando a los estudiantes para implementar programas de seguridad integrales en las organizaciones.

## 5. OBJETIVOS

- Comprender los principios y prácticas de la gestión de riesgos y la gobernanza de seguridad en las organizaciones.
- Planificar e implementar programas de ciberseguridad que aborden las necesidades de la organización.
- Gestionar la continuidad del negocio, la recuperación ante desastres y la seguridad del personal.

## 6. RESULTADOS DEL ESTUDIANTE

- 4) Reconocer las responsabilidades profesionales y tomar decisiones informadas en la práctica de la computación basadas en principios legales y éticos. (Assessment)
- 5) Funcionar efectivamente como miembro o líder de un equipo involucrado en actividades apropiadas a la disciplina del programa. (Usage)
- 6) Aplicar principios y prácticas de seguridad para mantener las operaciones en presencia de riesgos y amenazas. (Assessment)

## 7. TEMAS

Unidad 1: Gestión de riesgos (10 horas)	
Resultados esperados: 4,6	
Temas	Objetivos de Aprendizaje ( <i>Learning Outcomes</i> )
<ul style="list-style-type: none"> <li>● Identificación de riesgos <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>● Evaluación y análisis de riesgos. <ul style="list-style-type: none"> <li>– El análisis de riesgos es el proceso organizacional para determinar y abordar posibles pérdidas accidentales o intencionales.</li> <li>– Diseñar e implementar procedimientos para minimizar el impacto de estas pérdidas.</li> <li>– También puede abarcar análisis de amenazas e inteligencia de amenazas.</li> </ul> </li> <li>● Amenazas internas <ul style="list-style-type: none"> <li>– 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.</li> <li>– Una amenaza interna se define como el riesgo de que una persona interna utilice su acceso autorizado, consciente o inconscientemente, para dañar su organización.</li> <li>– 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.</li> <li>– Comportamientos motivo-medio-oportunidad: factores de motivación y disciplina, responsabilidad, conciencia y control de calidad.</li> <li>– El FBI ha desarrollado materiales que incluyen indicadores útiles para identificar posibles riesgos de amenazas internas.</li> </ul> </li> <li>● Modelos y metodologías de medición y evaluación de riesgos <ul style="list-style-type: none"> <li>– 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).</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>● Describir la gestión de riesgos y su papel en la organización [Usar]</li> <li>● Describir técnicas de gestión de riesgos para identificar y priorizar factores de riesgo para activos de información y cómo se evalúa el riesgo [Usar]</li> <li>● Analice las opciones de estrategia utilizadas para tratar el riesgo y esté preparado para seleccionar entre ellas cuando se le proporcione información general [Usar]</li> <li>● Describir metodologías populares utilizadas en la industria para gestionar el riesgo [Usar]</li> </ul>

Unidad 2: Gobernanza y política de seguridad (12 horas)	
Resultados esperados: 4,5,6	
Temas	Objetivos de Aprendizaje ( <i>Learning Outcomes</i> )
<ul style="list-style-type: none"> <li>• Contexto organizacional <ul style="list-style-type: none"> <li>– Las diferencias contextuales internas versus externas tienen un impacto importante en la cobertura de políticas, regulaciones y estatutos (o jurisdicción).</li> <li>– Se deben evaluar las cuestiones e inquietudes específicas de la ubicación o del país.</li> <li>– También se deben evaluar las normas y directrices aplicables para su cumplimiento por parte de la industria/sector.</li> <li>– 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.</li> <li>– Diferencia entre organizaciones en diversos segmentos industriales verticales de negocios, como energía versus agricultura.</li> </ul> </li> <li>• Privacidad <ul style="list-style-type: none"> <li>– Aborda las variaciones sociales y localizadas en la privacidad.</li> <li>– Se deben explorar las variaciones jurisdiccionales en las definiciones de privacidad.</li> <li>– También deben abordarse las relaciones entre individuos, organizaciones o los requisitos de privacidad gubernamentales.</li> <li>– 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.</li> </ul> </li> <li>• Leyes, ética y cumplimiento <ul style="list-style-type: none"> <li>– 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.</li> <li>– La instrucción ética también debería ser un elemento.</li> <li>– Deben abordarse los códigos de conducta profesionales y las normas éticas.</li> <li>– 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.</li> <li>– 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.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Discuta la importancia, los beneficios y los resultados deseados de la gobernanza de la ciberseguridad y cómo se implementaría dicho programa [Usar]</li> <li>• Describir la política de seguridad de la información y su papel en un programa de seguridad de la información exitoso [Usar]</li> <li>• Describa los principales tipos de políticas de seguridad de la información y los principales componentes de cada una [Usar]</li> <li>• Explique qué es necesario para desarrollar, implementar y mantener una política efectiva y qué consecuencias puede enfrentar la organización si no lo hace [Usar]</li> <li>• Diferenciar entre derecho y ética [Usar]</li> <li>• Identificar leyes nacionales e internacionales importantes que se relacionen con la ciberseguridad. [Usar]</li> <li>• Explicar cómo las organizaciones logran el cumplimiento de las leyes y regulaciones nacionales e internacionales, y de los estándares industriales específicos [Usar]</li> <li>• Se debe dar mayor consideración a la privacidad en el contexto de las regulaciones de protección al consumidor y atención médica [Usar]</li> <li>• 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]</li> <li>• Describa por qué los códigos de conducta éticos son importantes para los profesionales de la ciberseguridad y sus organizaciones [Usar]</li> </ul>

Unidad 3: Herramientas analíticas (8 horas)	
Resultados esperados: 4	
Temas	Objetivos de Aprendizaje ( <i>Learning Outcomes</i> )
<ul style="list-style-type: none"> <li>• Medidas de rendimiento (métricas) <ul style="list-style-type: none"> <li>– Se deben explicar a los estudiantes los enfoques y técnicas para definir y evaluar la utilidad de las mediciones del desempeño.</li> </ul> </li> <li>• Análisis de datos <ul style="list-style-type: none"> <li>– 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</li> <li>– Cómo funcionan las herramientas de análisis de seguridad</li> <li>– La relación entre el software y las herramientas analíticas y la ciencia forense.</li> <li>– Diferencias entre herramientas forenses y herramienta analítica</li> <li>– Análisis forense de red (para incluir análisis de paquetes, herramientas, Windows, Linux, UNIX, Mobile)</li> <li>– Diferencias entre ciberforense (redes sociales, por ejemplo) y forense de redes.</li> </ul> </li> <li>• Inteligencia de seguridad <ul style="list-style-type: none"> <li>– 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.</li> <li>– Ejemplos de fuentes de inteligencia de seguridad incluyen SIEM para datos internos y servicios de inteligencia públicos y privados para datos externos.</li> <li>– La difusión incluye una comprensión del enfoque del Centro de análisis e intercambio de información, así como de organizaciones como InfraGard.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Diferenciar entre derecho y ética [Usar]</li> <li>• Describa por qué los códigos de conducta éticos son importantes para los profesionales de la ciberseguridad y sus organizaciones [Usar]</li> <li>• Identificar leyes nacionales e internacionales importantes que se relacionen con la ciberseguridad. [Usar]</li> <li>• Explicar cómo las organizaciones logran el cumplimiento de las leyes y regulaciones nacionales e internacionales, y de los estándares industriales específicos [Usar]</li> </ul>
Lecturas : [NIST-SP800-137]	

Unidad 4: Administración de Sistemas (8 horas)	
Resultados esperados: 4,5,6	
Temas	Objetivos de Aprendizaje ( <i>Learning Outcomes</i> )
<ul style="list-style-type: none"> <li>● Administración del sistema operativo <ul style="list-style-type: none"> <li>– 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.</li> </ul> </li> <li>● Administración del sistema de base de datos. <ul style="list-style-type: none"> <li>– 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.</li> <li>– La cobertura debe incluir las tecnologías de almacenamiento de datos de uso generalizado, así como las tecnologías emergentes de gestión de datos.</li> </ul> </li> <li>● administración de red <ul style="list-style-type: none"> <li>– incluye, entre otros, el modelo OSI, protección del tráfico de red y herramientas para la configuración de servicios.</li> </ul> </li> <li>● administración de la nube <ul style="list-style-type: none"> <li>– Este tema incluye, entre otros, la configuración e implementación de aplicaciones y usuarios en infraestructuras de nube.</li> <li>– analizando el desempeño</li> <li>– escalamiento de recursos</li> <li>– disponibilidad de plataformas en la nube</li> <li>– identificar problemas de seguridad y privacidad y mitigar riesgos.</li> </ul> </li> <li>● Administración de sistemas ciberfísicos. <ul style="list-style-type: none"> <li>– Incluye, entre otros, la arquitectura de los sistemas ciberfísicos.</li> <li>– Estándares de comunicación subyacentes (Zigbee).</li> <li>– software intermedio</li> <li>– Arquitectura orientada a Servicios</li> <li>– Herramientas que soportan el control en tiempo real y la aplicación de ejemplos del mundo real (red eléctrica, instalación nuclear, IoT, SCADA).</li> </ul> </li> <li>● Endurecimiento del sistema <ul style="list-style-type: none"> <li>– incluye, entre otros, la identificación de riesgos, amenazas y vulnerabilidades en sistemas de uso común (sistemas operativos, sistemas de bases de datos, redes)</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>● Diferenciar entre derecho y ética [Usar]</li> <li>● Describa por qué los códigos de conducta éticos son importantes para los profesionales de la ciberseguridad y sus organizaciones [Usar]</li> <li>● Identificar leyes nacionales e internacionales importantes que se relacionen con la ciberseguridad. [Usar]</li> <li>● Explicar cómo las organizaciones logran el cumplimiento de las leyes y regulaciones nacionales e internacionales, y de los estándares industriales específicos [Usar]</li> </ul>

Unidad 5: Planificación de ciberseguridad (10 horas)	
Resultados esperados: 4,5	
Temas	Objetivos de Aprendizaje ( <i>Learning Outcomes</i> )
<ul style="list-style-type: none"> <li>• Planificación estratégica <ul style="list-style-type: none"> <li>– Cubre conceptos tales como determinar la posición actual de la organización.</li> <li>– 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.</li> <li>– asignar el presupuesto necesario</li> <li>– Implementar la estrategia en la organización y actualizarla y adaptarla anualmente.</li> </ul> </li> <li>• Gestión Operativa y Táctica <ul style="list-style-type: none"> <li>– 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.</li> <li>– Especial énfasis en la mejora de procesos y la gestión de la cadena de suministro.</li> <li>– Estrategias de operación</li> <li>– Estrategia táctica</li> <li>– Diseño de productos y servicios</li> <li>– Diseño y Análisis de procesos</li> <li>– Planificación de capacidad</li> <li>– Sistemas de producción lean</li> <li>– Gestión de materiales e inventarios</li> <li>– Gestión de calidad y seis sigma</li> <li>– Gestión de proyectos</li> <li>– Gestión de la cadena de suministro</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Explicar la planificación organizacional estratégica para la ciberseguridad y su relación con la planificación estratégica de TI y para toda la organización [Usar]</li> <li>• Identificar las partes interesadas clave de la organización y sus roles [Usar]</li> <li>• Describir los componentes principales de la planificación de la implementación del sistema de ciberseguridad [Usar]</li> </ul>
Lecturas : [Alberts2014]	

## 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